

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-133955

(43)Date of publication of application : 22.05.1998

(51)Int.Cl. G06F 12/14
G06F 12/00
G09C 1/00
H04L 9/08
H04L 9/14

(21)Application number : 08-286345

(71)Applicant : MATSUSHITA ELECTRIC IND
CO LTD

(22)Date of filing : 29.10.1996

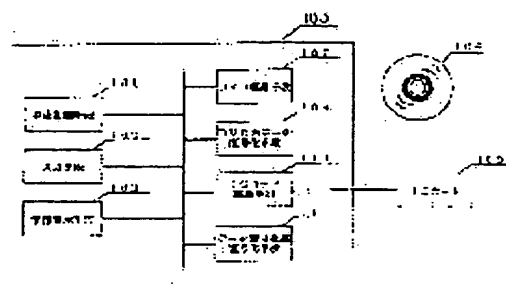
(72)Inventor : URANAKA SACHIKO
KIYONO MASAKI

(54) PORTABLE MEDIUM DRIVING DEVICE, ITS METHOD, COOPERATIVE DEVICE OF PORTABLE MEDIUM AND NETWORK, AND ITS METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To eliminate the illegal use of a portable medium at the time of using the portable medium individually or in cooperation with a network.

SOLUTION: Data ciphered by a data ciphering key D is recorded in the portable medium 106 and a ciphered data ciphering key ciphered by using a user's open key PU in an open key ciphering system is recorded at a part different from the original storing area of the medium 106. A portable medium reproducing device is provided with a means capable of obtaining the secret key PS of the user to decode a data ciphering key D by a data ciphering key decoding means 111 through the use of this key PS and to restore data within the medium 106 by an in-DVD data restoring means 108 through the use of this key D to display. In addition, by constituting to obtain a ciphered data ciphering key through the network, the using quantity or the using effective time limit of the medium 106 are managed, charging is executed and using is restricted.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-133955

(43) 公開日 平成10年(1998) 5月22日

| (51) Int.Cl. ⁸ | 識別記号 | F I |
|---------------------------|-------|-----------------------|
| G 0 6 F 12/14 | 3 2 0 | G 0 6 F 12/14 3 2 0 D |
| 12/00 | 5 3 7 | 12/00 5 3 7 H |
| G 0 9 C 1/00 | 6 6 0 | G 0 9 C 1/00 6 6 0 D |
| H 0 4 L 9/08 | | H 0 4 L 9/00 6 0 1 A |
| 9/14 | | 6 0 1 E |

審査請求 未請求 請求項の数24 O L (全 54 頁) 最終頁に続く

(21) 出願番号 特願平8-286345

(22) 出願日 平成8年(1996)10月29日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 浦中 祥子

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 清野 正樹

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

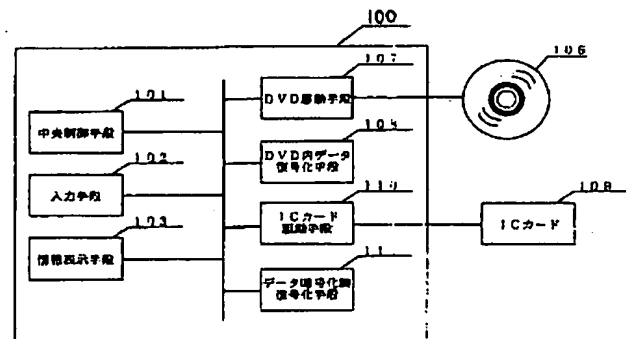
(74) 代理人 弁理士 滝本 智之 (外1名)

(54) 【発明の名称】 可搬型メディア駆動装置とその方法、及び可搬型メディアとネットワークの連携装置とその方法

(57) 【要約】

【課題】 可搬型メディアを単独で、あるいはネットワークと連携して用いる場合に、その不正使用を排除することを目的とする。

【解決手段】 可搬型メディア106にはデータ暗号化鍵Dで暗号化されたデータを記録しておき、可搬型メディア106の本来の記憶領域とは異なる部分に、公開鍵暗号方式における利用者の公開鍵PUを用いて暗号化された暗号化データ暗号化鍵を記録しておく。可搬型メディア再生装置には利用者の秘密鍵PSを取得できる手段を備えておき、この利用者秘密鍵PSを用いてデータ暗号化鍵復号化手段111によりデータ暗号化鍵Dを復号化し、さらにこのデータ暗号化鍵Dを用いてDVD内データ復号化手段108により可搬型メディア106内のデータを復元して表示する。また、ネットワークを通じて、暗号化データ暗号化鍵を取得する構成にすることにより、可搬型メディア106の使用量、あるいは使用有効期限を管理し、課金を施したり、使用を制限する。



【特許請求の範囲】

【請求項1】 それぞれに固有なメディア活用情報と、データ暗号化鍵によって暗号化された暗号化データとを記録し、前記メディア活用情報としては、データ暗号化鍵を、利用者ごとの秘密情報で復号可能な形式で暗号化した、暗号化データ暗号化鍵を少なくとも含んだ可搬型メディアから、前記暗号化データを解読する装置であり、その構成としては、前記可搬型メディアを駆動する可搬型メディア駆動手段と、利用者ごとの秘密情報を取得する秘密情報取得手段と、前記可搬型メディアに記録されている暗号化データを前記データ暗号化鍵を用いて復号化しデータを生成する第1のデータ復号化手段と、前記秘密情報取得手段で取得した利用者ごとの秘密情報を用いてメディア活用情報に含まれている前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成する第2のデータ復号化手段とを備え、利用者ごとの秘密情報と暗号化データ暗号化鍵とを用いて、可搬型メディア内の暗号化データを復号化してデータを生成することを特徴とする可搬型メディア駆動装置。

【請求項2】 それぞれに固有なメディア活用情報と、データ暗号化鍵によって暗号化された暗号化データとを記録し、前記メディア活用情報としては、データ暗号化鍵を、利用者ごとの秘密情報で復号可能な形式で暗号化した、暗号化データ暗号化鍵を少なくとも含んだ可搬型メディアから、前記暗号化データ暗号化鍵を得るステップと、前記ステップと同時にあるいはその前後に利用者ごとの秘密情報を得るステップと、前記得られた利用者ごとの秘密情報を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成するステップと、前記データ暗号化鍵を用いて、前記可搬型メディアに記録されている暗号化データを復号化してデータを生成するステップとからなる可搬型メディア駆動方法。

【請求項3】 それぞれに固有なメディア活用情報と、データ暗号化鍵によって暗号化された暗号化データとを記録した可搬型メディアと、前記暗号化データを解読する第1の電子計算機と、前記解読に必要な情報を前記第1の電子計算機に提供する第2の電子計算機と、前記第1と第2の電子計算機を繋ぐネットワークとから構成され、前記メディア活用情報としては、前記可搬型メディアに記録されているデータの種類に対応する情報であるタイトル情報と、前記可搬型メディアと他とを区別する情報である前記タイトル情報ごとの発行番号情報とを少なくとも含み、前記第1の電子計算機は、前記可搬型メディアを駆動する可搬型メディア駆動手段と、利用者ごとの秘密情報を

格納する第1の秘密情報格納手段と、前記可搬型メディアに記録されている暗号化データをデータ暗号化鍵を用いて復号化しデータを生成する第1のデータ復号化手段と、前記ネットワークに対する入出力を行なう第1の情報送受信手段と、前記利用者ごとの秘密情報を用いて復号化する第2のデータ復号化手段とを備え、前記第2の電子計算機は、前記可搬型メディアに記録されている暗号化データの暗号化に用いたデータ暗号化鍵を、タイトル情報ごとに管理する可搬型メディア情報管理手段と、前記第1の秘密情報格納手段に格納されている利用者ごとの秘密情報と一対の公開情報を、発行番号情報ごとに管理する利用者情報管理手段と、前記公開情報を用いてデータ暗号化鍵を暗号化して暗号化データ暗号化鍵を生成するデータ暗号化手段と、前記ネットワークに対する入出力を行なう第2の情報送受信手段とを備え、前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、前記データ暗号化手段によって生成された暗号化データ暗号化鍵を第2の電子計算機から第1の電子計算機に送信した後、前記第2のデータ復号化手段が前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成することを特徴とする可搬型メディアとネットワークの連携装置。

【請求項4】 第2の電子計算機が、任意のデータに対して、その時限りの疑似変化を与えることのできる疑似変化情報を生成する疑似変化情報生成手段を更に備え、データ暗号化手段が、前記疑似変化情報と公開情報とを用いて暗号化データ暗号化鍵を生成することを特徴とする請求項3に記載の可搬型メディアとネットワークの連携装置。

【請求項5】 第1の電子計算機において、それぞれに固有なメディア活用情報と、データ暗号化鍵によって暗号化された暗号化データとを記録し、前記メディア活用情報としては、前記可搬型メディアに記録されているデータの種類に対応する情報であるタイトル情報と、前記可搬型メディアと他とを区別する情報である前記タイトル情報ごとの発行番号情報とを少なくとも含んだ可搬型メディアから、前記タイトル情報と前記発行番号情報とを得るステップと、前記タイトル情報と前記発行番号情報とをネットワークを経由して第2の電子計算機に送信するステップと、前記第2の電子計算機において、前記タイトル情報と前記発行番号情報とを受信するステップと、前記タイトル情報から前記データ暗号化鍵を得るステップと、前記タイトル情報と前記発行番号情報とから、利用者ごとの秘密情報と一対の公開情報を得るステップと、任意のデータに対して、その時限りの疑似変化を与える疑似変化情報を生成するステップと、前記疑似変化情報と前記公開

情報とを用いて前記データ暗号化鍵を暗号化して暗号化データ暗号化鍵を生成するステップと、前記暗号化データ暗号化鍵を前記第1の電子計算機にネットワークを経由して送信するステップと、

前記第1の電子計算機において、前記暗号化データ暗号化鍵を受信するステップと、前記公開情報により変換されたデータに対して唯一復元可能な前記利用者ごとの秘密情報を得るステップと、前記秘密情報を用いて前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成するステップと、前記データ暗号化鍵を用いて可搬型メディアに記録されている暗号化データを復号化してデータを生成するステップとからなる可搬型メディアとネットワークの連携方法。

【請求項6】 それぞれに固有なメディア活用情報を記録した可搬型メディアと、第1の電子計算機と、第2の電子計算機と、前記第1と第2の電子計算機の間を結ぶネットワークとから構成され、

前記第1の電子計算機は、前記可搬型メディアを駆動する可搬型メディア駆動手段と、データを暗号化するデータ暗号化手段と、前記ネットワークに対する入出力を行なう第1の情報送受信手段とを備え、

前記第2の電子計算機は、それぞれに固有な秘密情報を格納する第2の秘密情報格納手段と、任意のデータに対して、その時限りの疑似変化を与える疑似変化情報を生成する疑似変化情報発生手段と、前記疑似変化情報など、情報を記憶する情報記憶手段と、データを復号化するデータ復号化手段と、前記ネットワークに対する入出力を行なう第2の情報送受信手段とを備え、

前記メディア活用情報としては、前記第2の秘密情報格納手段に格納された秘密情報と一対の公開情報が少なくとも含まれており、

前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、

前記データ暗号化手段が、前記第2の電子計算機より送信される疑似変化情報と前記メディア活用情報に含まれる公開情報とを用いて、データを暗号化し、暗号化データを生成し、

前記データ復号化手段が、前記情報記憶手段により記憶しておいた疑似変化情報と前記第2の秘密情報格納手段に格納されている秘密情報とを用いて前記データ暗号化手段によって生成された暗号化データの復号化を行うことを特徴とする可搬型メディアとネットワークの連携装置。

【請求項7】 第2の電子計算機において、第1の電子計算機の要求を受けて、任意のデータに対し、その時限りの疑似変化を与える疑似変化情報を生成するステップと、前記疑似変化情報を記憶し、前記第1の電子計算機にネットワークを経由して送信するステップと、

前記第1の電子計算機において、前記送信された疑似変

化情報を受信するステップと、可搬型メディアに記録されているメディア活用情報が含んでいる公開情報を得るステップと、前記疑似変化情報と前記公開情報とを用いてデータを暗号化して暗号化データを生成するステップと、前記暗号化データを前記第2の電子計算機にネットワークを経由して送信するステップと、

前記第2の電子計算機において、前記暗号化データを受信するステップと、前記公開情報により変換されたデータに対して唯一復元可能な、秘密情報を得るステップと、前記記憶しておいた疑似変化情報と秘密情報とを用いて暗号化データを復号化してデータを生成するステップとからなる可搬型メディアとネットワークの連携方法。

【請求項8】 それぞれに固有なメディア活用情報を記録した可搬型メディアと、第1の電子計算機と、第2の電子計算機と、前記第1と第2の電子計算機の間を結ぶネットワークとから構成され、

前記第1の電子計算機は、前記可搬型メディアを駆動する可搬型メディア駆動手段と、前記ネットワークに対する入出力を行なう第1の情報送受信手段とを備え、

前記第2の電子計算機は、前記可搬型メディアの使用量を管理する可搬型メディア使用量管理手段と、前記ネットワークに対する入出力を行なう第2の情報送受信手段とを備え、

前記メディア活用情報としては、前記可搬型メディア内のデータの種類に対応する情報としてのタイトル情報と、前記可搬型メディアと他とを区別する情報としての前記タイトル情報ごとの発行番号情報とが少なくとも含まれており、

前記可搬型メディア使用量管理手段が、前記第1の電子計算機から送信される前記タイトル情報と前記発行番号情報とを用いて可搬型メディアを特定して該メディアの使用量を管理することを特徴とする可搬型メディアとネットワークの連携装置。

【請求項9】 第1の電子計算機において、可搬型メディアに記録されているメディア活用情報に含まれているタイトル情報と発行番号情報とを得るステップと、前記タイトル情報と前記発行番号情報とを第2の電子計算機にネットワークを経由して送信するステップと、

前記第2の電子計算機において、前記使用量と前記タイトル情報と前記発行番号情報とを受信するステップと、前記タイトル情報の前記発行番号情報に対して既に使用量が記録されている場合には、前記使用量に対して、新たな使用量を加算するステップと、前記タイトル情報の前記発行番号情報に対して使用量が記録されていない場合には、前記タイトル情報の前記発行番号情報に対応するエントリを新たに作成し、該メディアの使用量として、前記使用量を記録するステップとからなる可搬型メディアとネットワークの連携方法。

【請求項10】 メディア使用量管理手段において、タ

イトル情報と発行番号情報に加え、該メディア内のデータ名などをも用いてデータごとの使用量を階層的に管理することを特徴とする、請求項8に記載の可搬型メディアとネットワークの連携装置。

【請求項11】 メディア使用量管理手段が、タイトル情報と発行番号情報ごとの使用量に加え、該可搬型メディアの最大使用量を管理し、使用量が最大使用量を超えているかどうかを判断することを特徴とする請求項8に記載の可搬型メディアとネットワークの連携装置。

【請求項12】 メディア活用情報の一部として、タイトル情報と発行番号情報に加え、該可搬型メディアの最大使用量を更に設け、前記タイトル情報の前記発行番号情報のデータ使用量がメディア使用量管理手段に記録されていない場合には、メディア活用情報に記録されている最大使用量をメディア使用量管理手段における前記タイトル情報の前記発行番号情報の最大使用量として記録することを特徴とする請求項11に記載の可搬型メディアとネットワークの連携装置。

【請求項13】 可搬型メディアが、メディア活用情報に加え、データ暗号化鍵によって暗号化された暗号化データを更に記録し、

第1の電子計算機が、利用者ごとの秘密情報を格納する第1の秘密情報格納手段と、前記暗号化データをデータ暗号化鍵を用いて復号化しデータを生成する第1のデータ復号化手段と、前記利用者ごとの秘密情報を用いて復号化する第2のデータ復号化手段とを更に備え、

第2の電子計算機が、前記可搬型メディアに記録されている暗号化データの暗号化に用いたデータ暗号化鍵を、タイトル情報ごとに管理する可搬型メディア情報管理手段と、前記公開情報を用いてデータ暗号化鍵を暗号化して暗号化データ暗号化鍵を生成するデータ暗号化手段とを更に備え、

可搬型メディア使用量管理手段が、前記可搬型メディアの使用量に加え、前記第1の秘密情報格納手段に格納されている利用者ごとの秘密情報と一対の公開情報も、発行番号情報ごとに管理しており、

前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、

可搬型メディアの使用量が最大使用量を超えていない場合、前記暗号化手段によって生成された暗号化データ暗号化鍵を第1の電子計算機から第2の電子計算機に送信した後、前記第2のデータ復号化手段が前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成することを特徴とする請求項11又は請求項12に記載の可搬型メディアとネットワークの連携装置。

【請求項14】 第1の電子計算機が、データを暗号化するデータ暗号化手段を更に備え、

第2の電子計算機が、それぞれに固有な秘密情報を格納

する第2の秘密格納手段と、任意のデータに対して、その時限りの疑似変化を与える疑似変化情報を生成する疑似変化情報生成手段と、前記疑似変化情報などの情報を記憶する情報記憶手段と、データを復号するデータ復号化手段とを更に備え、

可搬型メディアに記録されているメディア活用情報としては、前記第2の秘密情報格納手段に格納された秘密情報と一対の公開情報を更に含み、

前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、

前記データ暗号化手段が、前記第2の電子計算機より送信された疑似変化情報と前記メディア活用情報に含まれる公開情報を用いて、タイトル情報と発行番号情報とを暗号化し、

前記データ復号化手段が、前記情報記憶手段により記憶しておいた疑似変化情報と前記第2の秘密情報格納手段に格納されている秘密情報とを用いて、前記暗号化されたタイトル情報と発行番号情報とを復号化し、

可搬型メディア使用量管理手段が、前記復号化されたタイトル情報と発行番号情報とを用いて、可搬型メディアを特定して該メディアの使用量を管理することを特徴とする請求項8に記載の可搬型メディアとネットワークの連携装置。

【請求項15】 それぞれに固有なメディア活用情報を記録した可搬型メディアと、前記可搬型メディアを再生する第1の電子計算機と、前記可搬型メディアの使用期限を管理する第2の電子計算機と、前記第1と第2の電子計算機の間を結ぶネットワークとから構成され、前記メディア活用情報としては、前記可搬型メディア内のデータの種類に対応する情報としてのタイトル情報が少なくとも含まれており、

前記第1の電子計算機は、前記可搬型メディアを駆動する可搬型メディア駆動手段と、前記ネットワークに対する入出力を行なう第1の情報送受信手段とを備え、

前記第2の電子計算機は、前記タイトル情報によって特定される可搬型メディアの使用期限を管理する可搬型メディア使用期限管理手段と、前記特定される可搬型メディアが使用有効期限内であるかどうかを判断する使用有効期限判断手段と、前記ネットワークに対する入出力を行なう第2の情報送受信手段とを備え、

第1の電子計算機において可搬型メディアを使用する際に、タイトル情報を第2の電子計算機に送信し、第2の電子計算機において、各可搬型メディア毎に使用有効期限内であるかどうかを判断することを特徴とする可搬型メディアとネットワークの連携装置。

【請求項16】 第1の電子計算機において、可搬型メディアに記録されているメディア活用情報に含まれているタイトル情報を得るステップと、前記タイトル情報を第2の電子計算機にネットワークを経由して送信するス

トップと、

前記第2の電子計算機において、前記タイトル情報を受信するステップと、前記タイトル情報に該当するメディアの使用有効期限情報を得るステップと、前記使用有効期限情報に基づき、前記メディアが使用有効期限内であるかどうかを判断するステップとからなる可搬型メディアとネットワークの連携方法。

【請求項17】 メディア活用情報の一部として、タイトル情報に加え、タイトル情報ごとの発行番号情報も更に含み、

可搬型メディア使用有効期限管理手段は、前記タイトル情報ごとの発行番号情報によって可搬型メディアを特定し、

第1の電子計算機から第2の電子計算機にタイトル情報を送信する際に、発行番号情報も同時に送信し、タイトル情報ごとの発行番号情報によって使用有効期限を管理することを特徴とする請求項15に記載の可搬型メディアとネットワークの連携装置。

【請求項18】 メディア使用有効期限管理手段において、タイトル情報に加え、該メディア内のデータ名をも用いてデータごとの使用有効期限を階層的に管理することを特徴とする、請求項15に記載の可搬型メディアとネットワークの連携装置。

【請求項19】 それぞれに固有なメディア活用情報を記録した可搬型メディアと、前記可搬型メディアを再生する第1の電子計算機と、前記可搬型メディアの使用期限を管理する第2の電子計算機と、前記第1と第2の電子計算機の間を結ぶネットワークとから構成され、前記メディア活用情報としては、該可搬型メディアの有効期限を示す使用有効期限情報が少なくとも含まれており、

前記第1の電子計算機は、前記可搬型メディアを駆動する可搬型メディア駆動手段と、前記ネットワークに対する入出力を行なう第1の情報送受信手段とを備え、

前記第2の電子計算機は、該当する可搬型メディアが使用有効期限内であるかどうかを判断する可搬型メディア使用有効期限判断手段と、前記ネットワークに対する入出力を行なう第2の情報送受信手段とを備え、

第1の電子計算機において可搬型メディアを使用する際に、前記メディア活用情報に含まれる使用有効期限情報を第2の電子計算機に送信し、第2の電子計算機において該可搬型メディアが使用有効期限内かどうかを判断することを特徴とする可搬型メディアとネットワークの連携装置。

【請求項20】 第1の電子計算機において、可搬型メディアに記録されおり、前記可搬型メディアにそれぞれ固有なメディア活用情報に含まれている前記可搬型メディアの使用有効期限情報を得るステップと、前記使用有効期限情報を第2の電子計算機にネットワークを経由して送信するステップと、

前記第2の電子計算機において、前記使用有効期限情報を受信するステップと、前記使用有効期限情報に基づき、前記可搬型メディアが使用有効期限内であるかどうか判断するステップとからなる可搬型メディアとネットワークの連携方法。

【請求項21】 メディア活用情報の一部として、可搬型メディア内に記録されている各データごとの使用有効期限情報を階層的に設け、メディア使用有効期限判断手段が、各データごとに使用有効期限内であるかどうかを判断することを特徴とする請求項19に記載の可搬型メディアとネットワークの連携装置。

【請求項22】 可搬型メディアが、メディア活用情報に加え、データ暗号化鍵によって暗号化された暗号化データを更に記録し、

第1の電子計算機が、利用者ごとの秘密情報を格納する第1の秘密情報格納手段と、前記暗号化データをデータ暗号化鍵を用いて復号化しデータを生成する第1のデータ復号化手段と、前記利用者ごとの秘密情報を用いて復号化する第2のデータ復号化手段とを更に備え、

第2の電子計算機が、前記暗号化データの暗号化に用いたデータ暗号化鍵を管理する可搬型メディア情報管理手段と、前記利用者ごとの秘密情報と一対の公開情報を管理する利用者情報管理手段と、前記公開情報を用いてデータ暗号化鍵を暗号化して暗号化データ暗号化鍵を生成するデータ暗号化手段とを更に備え、

前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、

前記可搬型メディアの使用有効期限内である場合、前記暗号化手段によって生成された暗号化データ暗号化鍵を第1の電子計算機から第2の電子計算機に送信した後、前記第2のデータ復号化手段が前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成することを特徴とする請求項19又は請求項21に記載の可搬型メディアとネットワークの連携装置。

【請求項23】 可搬型メディアが、メディア活用情報に加え、データ暗号化鍵によって暗号化された暗号化データを更に記録し、

第1の電子計算機が、利用者ごとの秘密情報を格納する第1の秘密情報格納手段と、前記暗号化データをデータ暗号化鍵を用いて復号化しデータを生成する第1のデータ復号化手段と、前記利用者ごとの秘密情報を用いて復号化する第2のデータ復号化手段とを更に備え、

第2の電子計算機が、前記暗号化データの暗号化に用いたデータ暗号化鍵を、タイトル情報ごとに管理する可搬型メディア管理手段と、前記利用者ごとの秘密情報と一対の公開情報を管理する利用者情報管理手段と、前記公開情報を用いてデータ暗号化鍵を暗号化して暗号化データ暗号化鍵を生成するデータ暗号化手段とを更に備え、前記公開情報と前記秘密情報とは、公開情報を用いてデ

ータを変換すると、秘密情報を用いてしか復元できない関係にあり、

第2の電子計算機の使用有効期限管理手段によって、第1の電子計算機より送信されるタイトル情報に該当する可搬型メディアが、使用有効期限内であると判断された場合にのみ、前記データ暗号化手段によって生成される暗号化データ暗号化鍵を、前記第2の電子計算機から前記第1の電子計算機へ送信し、前記第2のデータ復号化手段が前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵を生成することを特徴とする、請求項15に記載の可搬型メディアとネットワークの連携装置。

【請求項24】 第1の電子計算機が、データを暗号化するデータ暗号化手段を更に備え、
第2の電子計算機が、それぞれに固有な秘密情報を格納する第2の秘密情報格納手段と、任意のデータに対して、その時限りの疑似変化を与える疑似変化情報を生成する疑似変化情報生成手段と、前記疑似変化情報など、情報を記憶する情報記憶手段と、データを復号化するデータ復号化手段とを更に備え、
メディア活用情報としては、前記秘密情報と一対の公開情報が少なくとも含まれており、
前記公開情報と前記秘密情報とは、公開情報を用いてデータを変換すると、秘密情報を用いてしか復元できない関係にあり、
タイトル情報を第2の電子計算機に送信する際に、前記データ暗号化手段が、第2の電子計算機の生成する疑似変化情報と前記メディア活用情報に含まれる公開鍵情報とを用いて暗号化し、
前記データ復号化手段が、前記情報記憶手段により記憶しておいた前記疑似変化情報と前記第2の秘密情報格納手段に格納されている秘密情報とを用いて前記暗号化されたタイトル情報を復号化し、
前記復号化されたタイトル情報により特定される可搬型メディアが使用有効期限内であるかどうかを判断することを特徴とする、請求項15に記載の可搬型メディアとネットワークの連携装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、大量に出版される電子計算機用の可搬型メディア内に記録されている情報を、可搬型メディアの不正な利用を防止するために用いる、可搬型メディアに対するサービスの提供法、また、可搬型メディアとネットワークを連携させたサービスの提供法に関する。

【0002】

【従来の技術】従来、電子計算機用の可搬型メディアとしてはフロッピーディスクやCD-ROM、PDなどが利用されてきており、これらの不正な利用を防止するためのサービスの例として、CD-ROMのパッケージにキーコードのラベルを貼付しておき、利用開始時にこの

キーコードを入力させることにより、正しく購入したものであることを利用者自身に証明させるといったものがある。

【0003】また、ネットワークと連携したサービスとしては、特開平7-295674号公報に示すように、CD-ROMに一部暗号化されたデータを入れておき、ネットワーク等で別途入手する復号用の鍵でデータを解読して用い、同時に課金を行うシステムが提供されている。この方法について以下に簡単に説明する。

【0004】まず、そのセッションに限り有効な暗号化鍵を利用者の側で生成する。次に、この暗号化鍵をデータ復号用の鍵を配布するセンター側の公開鍵で暗号化してセンターに渡し、センターではセンターの秘密鍵を用いて利用者の側で生成した暗号化鍵を復号化し、この利用者が生成した暗号化鍵を用いてCD-ROM内のデータ復号用の鍵を暗号化して利用者へ送信する。この場合、センター側の公開鍵はCD-ROMにあらかじめ記録されている。このようにして、データ復号用の鍵の入手を安全に行うことを可能とするものである。

【0005】データ復号用の鍵の入手については、可搬型メディア上のデータの復号の場合に限らず、特開平7-288519号公報にあるように、公開鍵暗号方式を用いて相互に認証しながら交換する方法も提案されている。この方法について以下に簡単に説明する。

【0006】まず、利用者側から利用者の識別番号を送信するとともにデジタル情報をセンターに要求する。センターでは、識別番号に応じて管理しているパスワード、あるいは要求の時点で生成する乱数などをセンターの秘密鍵で署名して利用者へ返す。利用者の側では受けとったデータをセンターの公開鍵で認証して、通信相手が正しい相手であることを確認したうえで、解読済みのデータを利用者の秘密鍵で署名し、かつ、センターの公開鍵で暗号化してセンターに渡す。センターの側では、受けとったデータをセンターの秘密鍵で解読したうえで、さらに利用者の公開鍵で認証して、通信相手が正しい相手であることを確認したうえで、そのセッションに限り有効なセッション鍵を用いてデータを暗号化して利用者へ渡す。

【0007】また、特開平8-54951号公報に示すように、可搬型メディア上に限らず、ソフトウェアの使用量を検知して、最大可能使用量を超えた場合に、その使用を阻害する方法が提案されている。この方法について以下に簡単に説明する。

【0008】ソフトウェアの使用量を管理する手段を設け、ソフトウェアの使用量を検知し、予め定められた使用量に達したかどうかを判断し、規定の使用量を超えた場合には、ソフトウェアの出力信号を阻害する信号を重畳するなどして、使用を阻害する。または、あらかじめ出力信号を阻害するような信号を重畳したデータを記録しておき、規定された使用量を超えていない場合には、

阻害信号をはずして出力する。

【0009】また、一般に、試用期限が設けられたソフトウェアが配布されており、特定の期間に限って、ソフトウェアを試用することが可能で、その期間を過ぎると使用不可となるものがある。

【0010】

【発明が解決しようとする課題】しかし、CD-ROMのパッケージにキーコードのラベルを貼付する方法では、キーコードが誰の目にも明らかであり、CD-ROMを不正に貸与した場合にでも、このキーコードを入力しさえすればCD-ROMが利用できてしまうことになる。

【0011】また、特開平7-295674号公報に示す方法では、センターの公開鍵がCD-ROMの本体に記録されていることにより、公開鍵があらかじめ固定されることになり、課金処理を行うセンターを追加すると、その公開鍵を得るためには別途利用者が公開鍵取得の操作をすることが必要となるため、センターの追加のために利用者の利便性を損なう結果となる。しかし、逆に、センターの数をあらかじめ決定した数で抑えようとすると、センターが処理の集中に耐えられなくなる可能性もあり、利用者の利便性はやはり損なわれる結果となる。また、センターがクレジットカード会社を兼ねている場合には、あらかじめ固定されたセンターでしか運用しないとすると、利用者が既に持っているクレジットカードが使えない可能性があるという点で利用者の利便性を損なうものである。

【0012】逆に、複数のセンターを設けるためには、異なる金型を作成してCD-ROMをプレスする必要がある、その結果、コスト高を招くことになる。また、データ復号用の鍵を暗号化する特定セッション用の暗号化鍵を利用者側で生成してセンターに送る方法では、利用者認証が行なえず、CD-ROMを不正に貸与する可能性を排除できない。

【0013】特開平7-288519号公報では、利用者・センターの相互の認証の問題は解決されているが、センターの公開鍵を利用者側で得る方法については記述されていない。

【0014】また、特開平8-54951号公報にあるような方法では、利用者がこの方式によらずデータにアクセスすれば使用量を超過してもデータの利用が可能になるという可能性があるとともに、この方式によらなければアクセスできない形式のデータのみを提供することになるとすれば、汎用性に欠けるデータを配布することになる。

【0015】また、ソフトウェアの試用期間を限定する現在の方法では、パソコン側の時計を過去に戻したり、再度試用ソフトウェアをインストールしなおしたりといった方法で、再度試用可能な状態にすることができてしまい、事実上、特定期間に限定することが不可能であ

る。

【0016】本発明は、上記問題点に鑑み、可搬型メディアを単独で、あるいはネットワークと連携して用いる場合に、その不正使用を排除することを目的としてなされたものである。

【0017】

【課題を解決するための手段】上記の課題を解決するために、本発明は、第1に、大容量のデータの記録が可能な可搬型メディア内の暗号化データを復号化するのに必要なデータ暗号化鍵を利用者ごとの秘密情報で解読可能な形式で暗号化して、暗号化データ暗号化鍵とし、この暗号化データ暗号化鍵を、該可搬型メディアそれぞれに固有なメディア活用情報として記録しておき、利用者ごとの秘密情報は別途格納しておくことを特徴とする可搬型メディアの駆動装置であり、可搬型メディア内の暗号化データを復号化する際には、まず利用者ごとの秘密情報を得て、これによって可搬型メディアのメディア活用情報内の暗号化データ暗号化鍵を復号化してデータ暗号化鍵とし、さらにこのデータ暗号化鍵によって可搬型メディア内の暗号化データを復号化する構成としたものである。

【0018】これにより、可搬型メディアを利用できるのは、あらかじめ特定された利用者であって、かつ、利用の際には利用者ごとの秘密情報を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止するという効果を奏するものである。

【0019】また、本発明は、第2に、大容量のデータの記録が可能な可搬型メディア内の暗号化データを復号化するのに必要なデータ暗号化鍵を、可搬型メディアのメディア活用情報に記録されているタイトル情報ごとにサーバ側で管理しておき、また、利用者の秘密情報と一対の公開の情報を前記タイトル情報とタイトル情報ごとの発行番号情報ごとにサーバ側で管理しておき、利用者の秘密情報は別途格納しておいてクライアント側で利用することを特徴とする可搬型メディアとネットワークの連携装置であり、利用者はメディア活用情報に記録されているタイトル情報と発行番号情報をサーバ側に通知してデータ暗号化鍵の取得を依頼し、サーバ側は得られたタイトル情報に対応するデータ暗号化鍵を、得られたタイトル情報と発行番号情報に対応する公開の情報と、別途発生させる乱数などを用いて暗号化して送り返し、利用者側では利用者ごとの秘密情報を用いて、得られたデータから乱数を分離し、さらにデータ暗号化鍵を得て、暗号化データを復号化して利用する構成としたものである。

【0020】これにより、可搬型メディアを利用できるのは、タイトル情報・発行番号情報と、利用者の保持す

る秘密情報と一対の公開の情報を登録済みの特定された利用者であって、かつ、利用の際には利用者ごとの秘密情報を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止するとともに悪意の利用者のなりすましを防止できるという効果をも奏するものである。

【0021】また、本発明は、第3に、可搬型メディアのメディア活用情報にサーバの秘密情報と一対の公開情報を記録しておき、サーバの秘密情報は別途格納しておいてサーバ側で利用することを特徴とする可搬型メディアとネットワークの連携装置であり、利用者からサーバにデータを送信する際には、サーバで別途発生させる乱数などと、メディア活用情報内の公開情報を用いて暗号化して送信し、サーバ側では、サーバの秘密情報と前記乱数を用いて得られたデータの正当性を確認したのち、乱数を分離して、利用者からデータを得る構成としたものである。

【0022】これにより、利用者からサーバに安全にデータを送信する際に必要とする、サーバの公開鍵の取得が容易であるという効果を奏するものであり、かつ、サーバの公開鍵が可搬型メディアごとに異なるものであっても良いという効果を奏するものである。

【0023】また、本発明は、第4に、可搬型メディアそれぞれに固有のメディア活用情報としてタイトル情報とタイトル情報ごとの発行番号情報を設け、このタイトル情報と発行番号情報とを用いてサーバ側で可搬型メディアの使用量を管理することを特徴とする可搬型メディアとネットワークの連携装置であり、可搬型メディアを利用する際には、メディア活用情報内のタイトル情報と発行番号情報とをサーバに送信し、サーバ側では該可搬型メディアの使用量を加算したり、また、最大使用量が設定されている場合には、それを超えるかどうかの判断を行なう構成としたものである。

【0024】これにより、該可搬型メディアの使用量をもとに利用料金を利用者に対して請求したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた最大使用量を超える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止するという効果を奏するものである。

【0025】また、本発明は、第5に、前記第2の構成と前記第4の構成とを組合せた可搬型メディアとネットワークの連携装置であり、常にデータ暗号化鍵をサーバから取得するようにし、最大使用量を超える場合にはデータ暗号化鍵を渡さないようにする構成としたものである。

【0026】これにより、最大使用量を超えての可搬型メディアの無制限な利用を確実に防止するという効果を

奏するものである。

【0027】また、本発明は、第6に、前記第3の構成と前記第5の構成とを組合せた可搬型メディアとネットワークの連携装置であり、データ暗号化鍵取得のためのメディア活用情報を暗号化して送信する構成としたものである。

【0028】これにより、メディア活用情報に記述されている情報を安全にサーバに送信することが可能であるという効果を奏するものである。

【0029】また、本発明は、第7に、可搬型メディアそれぞれに固有のメディア活用情報として使用有効期限情報を設け、サーバ側には使用有効期限を判断する手段を設けたことを特徴とする可搬型メディアとネットワークの連携装置、あるいは、可搬型メディアそれぞれに固有のメディア活用情報としてタイトル情報、あるいはタイトル情報とタイトル情報ごとの発行番号情報とを設け、サーバ側にはタイトル情報、あるいはタイトル情報とタイトル情報ごとの発行番号情報とによって該可搬型メディアの使用有効期限を管理する手段と、使用有効期限を判断する手段を設けたことを特徴とする可搬型メディアとネットワークの連携装置であって、可搬型メディアを利用する際には、メディア活用情報内の使用有効期限情報、あるいはタイトル情報、あるいはタイトル情報と発行番号情報とをサーバに送信し、サーバ側で該可搬型メディアが使用可能かどうかを判断することを特徴としたものである。

【0030】これにより、可搬型メディアに対してあらかじめ使用有効期限を設定した場合に、それを超えて該可搬型メディアを利用しようとする場合にその旨通知したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた利用期間を超える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止するという効果を奏するものである。

【0031】また、本発明は、第8に、前記第2の構成と前記第7の構成とを組合せた可搬型メディアとネットワークの連携装置であり、常にデータ暗号化鍵をサーバから取得するようにし、使用有効期限を超える場合にはデータ暗号化鍵を渡さないようにする構成としたものである。

【0032】これにより、使用有効期限を超えての可搬型メディアの無制限な利用を確実に防止するという効果を奏するものである。

【0033】また、本発明は、第9に、前記第3の構成と前記第8の構成とを組合せた可搬型メディアとネットワークの連携装置であり、データ暗号化鍵取得のためのメディア活用情報を暗号化して送信する構成としたものである。

【0034】これにより、メディア活用情報に記述されている情報を安全にサーバに送信することが可能であるという効果を奏するものである。

【0035】

【発明の実施の形態】以下、本発明の実施の形態について、図1から図49を用いて説明する。

【0036】（実施の形態1）まず、請求項1及び2に対応する第1の実施の形態について説明する。図1は、本実施の形態における、可搬型メディアとして映画作品を記録した、映画作品再生システムの構成を示す図である。ここでは可搬型メディアとしては読み出し専用型デジタル・ヴァーサタイル・ディスク（Digital Versatile Disk、以下DVDと略す）を用い、可搬型メディアそれぞれに固有であるメディア活用情報は、DVD内の本来の記録領域とは異なる、DVD上の専用の箇所に記録する。この専用の箇所のことをメディア活用情報記録領域と今後称する。図1において、100はDVD再生装置である。101はDVD再生装置100の動作全体を制御する中央制御手段、102はDVD再生装置100に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、103は利用者に対してDVD再生装置100が表示を行なうためのディスプレイ、スピーカなどの情報表示手段である。106は映画作品をデータ暗号化鍵Dで暗号化して記録した映画作品DVDであって、そのメディア活用情報記録領域には、映画作品の暗号化に用いたデータ暗号化鍵Dを、公開鍵暗号方式における利用者の公開鍵によって暗号化した暗号化データ暗号化鍵が記録されている。107は映画作品DVD106を駆動するDVD駆動手段である。108は前記データ暗号化鍵Dを用いて映画作品DVD106内の暗号化された映画作品を復号化するDVD内データ復号化手段である。109は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているICカード、110はICカード109を駆動するICカード駆動手段である。111は前記利用者の秘密鍵を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵Dを生成するデータ暗号化鍵復号化手段である。

【0037】図2は、本実施の形態におけるメディア活用情報の構成例である。図2において、200はそれぞれに固有なメディア活用情報、203はメディア活用情報200のうち、前記暗号化データ暗号化鍵Dに関する情報を含むデータ暗号化鍵情報であり、映画作品DVD配布時には既にそのメディア活用情報記録領域に記録済みである。

【0038】図3は本実施の形態の処理の流れを示すフローチャートである。以下、図1から図3を用いて本実施の形態の動作を説明する。

【0039】利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品DVD106を入手する。特に、書店や通信販売による場合は、メディア活用情報記録領域に、利用者の

公開鍵で暗号化したデータ暗号化鍵Dを記録してもらったうえで購入する。会員制のサービスの場合には、あらかじめ公開鍵を登録して入会することにより、データ暗号化鍵Dを利用者の公開鍵で暗号化したもののメディア活用情報記録領域に記録した上で、配布してもらうことが容易に行なえる。

【0040】以降、利用者が映画作品DVDを再生する場合について、図3のフローチャートに沿って説明する。なお、図3においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、矢印は処理の流れを示している。

【0041】図3において、まず、利用者は、映画作品DVD106をDVD再生装置100のDVD駆動手段107にセットし、入力手段102を用いて、再生開始をDVD再生装置100の中央制御手段101に指示する。これにより、開始300に示すように、映画作品DVDの再生が開始される。

【0042】次に、ステップ301に示すように、中央制御手段101は映画作品DVD再生開始の指示を受け付け、ステップ302に進む。

【0043】次に、ステップ302に示すように、中央制御手段101の指示に従い、DVD駆動手段107は、映画作品DVD106のメディア活用情報記録領域から、データ暗号化鍵情報203を得て、ステップ303に進む。このデータ暗号化鍵情報203の中には、映画作品DVD内の映画作品の暗号化に用いたデータ暗号化鍵Dを、利用者の公開鍵で暗号化した、暗号化データ暗号化鍵が入っている。

【0044】次に、ステップ303に示すように、中央制御手段101の指示に従い、ICカード駆動手段110は、ICカード109に格納されている利用者の秘密鍵SUを得て、ステップ304に進む。

【0045】次に、ステップ304に示すように、中央制御手段101の指示に従い、データ暗号化鍵復号化手段111は、既に得た利用者の秘密鍵SUを用いて、データ暗号化鍵情報203に入っている暗号化データ暗号化鍵を復号化し、データ暗号化鍵Dを得て、ステップ305に進む。

【0046】次に、ステップ305に示すように、中央制御手段101の指示に従い、DVD内データ復号化手段108は、既に得たデータ暗号化鍵Dを用いて、映画作品DVD106上の暗号化されているデータを復号化し、情報表示手段103によって利用者に表示し、終了306へ進む。

【0047】なお、本実施の形態においては可搬型メディアとしてDVD、メディア活用情報の記録領域としてDVD上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやPD、CD-R OMなどの他のメディアや、書換え可能型のDVDを用

い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【0048】また、本実施の形態においては、利用者の秘密鍵をICカードに格納する例について示したが、ICカードへのアクセス時には、ICカード自身に設けられているパスワードなどを別途用いて、利用者以外の第三者からのアクセスを排除することも可能である。さらに、利用者の秘密鍵はICカードに格納するのではなく、DVD再生装置自身の記憶領域に暗号化して記録しておき、利用者のパスワード入力などによって復号化して利用するといった形態や、磁気カードに記録しておくといった形態、利用者自身が覚えておいて、都度入力するといった形態も可能である。

【0049】また、本実施の形態においては特に述べなかったが、映画作品DVDの中に複数の映画作品が記録されている場合に、データ暗号化鍵を映画作品ごとに設けることも可能である。その場合には、それぞれのデータ暗号化鍵を利用者の公開鍵で暗号化し、暗号化データ暗号化鍵をメディア活用情報記録領域に記録することになる。

【0050】また、本実施の形態においては、利用者を一人であると仮定していたが、家族など、複数の利用者が映画作品DVDを利用するということがあらかじめ分かっている場合には、複数の利用者それぞれの公開鍵によってデータ暗号化鍵を暗号化し、メディア活用情報記録領域に記録することによって、それぞれの利用者による映画作品DVDの利用を可能とすることができる。

【0051】また、本実施の形態においては特に述べなかったが、データ暗号化鍵や利用者の秘密鍵の漏洩を防止するために、ICカード駆動手段110、データ暗号化鍵復号化手段111は、情報表示手段103を実現するハードウェアに組み込むことによって実装してもよい。

【0052】以上のように、本実施の形態では、可搬型メディアを利用できるのは、あらかじめ特定された利用者であって、かつ、利用の際には利用者ごとの秘密情報を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止できる。

【0053】また、メディア活用情報は、可搬型メディアの金型でプレスするものではないため、大量に同一の内容を持つ可搬型メディアをプレスしたあとに、一枚ごとにメディア活用情報を記録することで、暗号化データのプレスのためには共通の金型を用いることができるというコスト低下にもつながり、その実用的効果は大きい。

【0054】（実施の形態2）次に、請求項3乃至5に対応する第2の実施の形態について説明する。図4は、

本実施の形態における、可搬型メディアとして映画作品を記録した、映画作品再生システムの構成を示す図である。なお、可搬型メディアとしては実施の形態1と同じ、読み出し専用型DVDを用いるものとする。

【0055】図4において、400はDVD再生装置である。401はDVD再生装置400の動作全体を制御する中央制御手段、402はDVD再生装置400に対して利用者が力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、403は利用者に対してDVD再生装置400が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、404はDVD再生装置400のネットワークに対する情報の送受信を行なう情報送受信手段である。406は映画作品をデータ暗号化鍵Dで暗号化して記録した映画作品DVDであって、そのメディア活用情報記録領域には、映画作品DVDの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報が記録されている。407は映画作品DVD406を駆動するDVD駆動手段である。408はデータ暗号化鍵Dを用いて前記映画作品DVD406内の暗号化された映画作品を復号化するDVD内データ復号化手段である。409は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているICカード、410はICカード409を駆動するICカード駆動手段である。411は前記利用者の秘密鍵を用いて、送信データ暗号化手段432によって生成される暗号化データ暗号化鍵を復号化してデータ暗号化鍵Dを生成するデータ暗号化鍵復号化手段である。

【0056】420は映画作品DVD406に記録されている映画作品の暗号化に用いたデータ暗号化鍵を管理し、利用者の要求に応じてデータ暗号化鍵を配布する鍵管理サーバである。421は前記鍵管理サーバ420の動作全体を制御する中央制御手段、424は鍵管理サーバ420のネットワークに対する情報の送受信を行なう情報送受信手段である。432は利用者に対して送信するデータ暗号化鍵を公開鍵暗号方式における利用者の公開鍵で暗号化する、すなわち暗号化データ暗号化鍵を生成する送信データ暗号化手段、433は送信データ暗号化手段において利用する乱数を発生させる乱数発生手段、434は利用者の公開鍵を、前記タイトル情報と前記発行番号情報によって管理する利用者情報管理手段、435は前記データ暗号化鍵を前記タイトル情報によって管理するDVD情報管理手段である。440はDVD再生装置400と鍵管理サーバ420との間を繋ぐネットワークである。

【0057】図5は、本実施の形態にかかわるメディア活用情報の構成例である。図5において、500はそれぞれに固有なメディア活用情報、メディア活用情報500のうち、501は映画作品DVDの種類を特定可能なタイトル情報、502は該映画作品DVDを他のものと

識別可能な、前記タイトル情報ごとの発行番号情報であり、映画作品DVD配布時には既に、前記メディア活用情報記録領域に記録済みである。

【0058】図6は、本実施の形態にかかわる利用者情報の構成例である。図6において、600は利用者情報、601はメディア活用情報500に含まれるタイトル情報、602はメディア活用情報500に含まれる発行番号情報、603はタイトル情報601と発行番号情報602とで特定可能な映画作品DVDを保有している利用者の、公開鍵暗号方式における公開鍵を含む、利用者公開鍵情報である。なお、ここでは、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは利用者情報管理手段434によって管理されている。

【0059】図7は、本実施の形態にかかわるDVD情報の構成例である。図7において、700はDVD情報、701はメディア活用情報500内に含まれるタイトル情報、702はこのタイトル情報701によって特定可能な種類の映画作品DVD内に記録されている映画作品を暗号化するのに用いたデータ暗号化鍵Dを含むデータ暗号化鍵情報である。なお、ここでは、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらはDVD情報管理手段435によって管理されている。

【0060】図8は本実施の形態の処理の流れを示すフローチャートである。以下、図4から図8を用いて本実施の形態の動作を説明する。

【0061】利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品DVD406を入手する。以降、利用者が映画作品DVDを再生する場合について、図8のフローチャートに沿って説明する。なお、図8においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、矢印は処理の流れを示している。

【0062】まず、利用者は、映画作品DVD406をDVD再生装置400のDVD駆動手段407にセットし、入力手段402を用いて、再生開始をDVD再生装置400の中央制御手段401に指示する。これにより、開始800に示すように、映画作品DVDの再生が開始される。

【0063】次に、ステップ801に示すように、DVD再生装置400の中央制御手段401は映画作品DVD再生開始の指示を受け付け、DVD駆動手段407によって映画作品DVD406のメディア活用情報500のうち、タイトル情報501と発行番号情報502とを得て、これらを情報送受信手段404により、ネットワーク440を経由して鍵管理サーバ420に送信し、暗号化データ暗号化鍵の取得を依頼し、ステップ802に進む。

【0064】次に、ステップ802に示すように、鍵管理サーバ420の中央制御手段421は、暗号化データ暗号化鍵取得依頼の指示を、タイトル情報501と発行番号情報502とともに情報送受信手段424により受信し、DVD情報管理手段435によって、タイトル情報501を元に、データ暗号化鍵情報702を得て、ステップ803に進む。ここで、DVD情報700のうちのタイトル情報701は、前記タイトル情報501と等しい値を持つ。

【0065】次に、ステップ803に示すように、利用者情報管理手段434によって、タイトル情報501と発行番号情報502とを元に、利用者公開鍵情報603を得て、ステップ804に進む。ここで、利用者情報600のうちのタイトル情報601と発行番号情報602とは、それぞれ前記タイトル情報501と前記発行番号情報502とに等しい。

【0066】次に、ステップ804に示すように、乱数発生手段433により、乱数Rを発生させ、ステップ805に進む。

【0067】次に、ステップ805に示すように、送信データ暗号化手段432において、前記乱数Rを用いて、前記データ暗号化鍵情報702に含まれているデータ暗号化鍵Dを暗号化し、さらに、Rと前記暗号化されたDとを組合せたデータを前記利用者公開鍵情報603に含まれている利用者公開鍵PUによって暗号化し、その結果を、情報送受信手段424により、ネットワーク440を経由してDVD再生装置400に送信し、ステップ806に進む。ここで、乱数Rと利用者公開鍵PUによる暗号化の関数を、それぞれ e_1 、 e_2 として、暗号化の様子を模式的に表すと、DVD再生装置400に送信されるデータは次の(数1)のようになる。 e_1 、 e_2 の引数は、それぞれ、一つ目の引数が暗号化鍵、二つ目の引数が暗号化されるデータである。

【0068】

【数1】 $e_2(PU, R + e_1(R, D))$

次に、ステップ806に示すように、DVD再生装置400は情報送受信手段404により鍵管理サーバ420からの(数1)で示されるデータを受信し、さらに、中央制御手段401の指示に従い、ICカード駆動手段410は、ICカード409に格納されている利用者秘密鍵SUを得て、データ暗号化鍵復号化手段411により、データ暗号化鍵Dを得て、ステップ807に進む。ここで、乱数Rと利用者秘密鍵SUによる復号化の関数を、それぞれ d_1 、 d_2 として、復号化の様子を模式的に表すと、データ暗号化鍵復号化手段の動作は以下の

(数4)から(数5)のように表される。 d_1 、 d_2 の引数は、それぞれ、一つ目の引数が暗号化鍵、二つ目の引数が復号化されるデータであり、前記暗号化の関数 e_1 、 e_2 とは、逆の関係にあり、それぞれ(数2)と(数3)に示すような関係がある。この式に現れるX、

Yは暗号化される対象のデータを示す変数である。

【0069】

【数2】 $d1(R, e1(R, X)) = X$

【0070】

【数3】 $d2(SU, e2(PU, Y)) = Y$

【0071】

【数4】 $d2(SU, e2(PU, R + e1(R, D))) = R + e1(R, D)$

【0072】

【数5】 $d1(R, e1(R, D)) = D$

次に、ステップ807に示すように、DVD内データ復号化手段408は、既に得たデータ暗号化鍵Dを用いて、映画作品DVD406の暗号化されているデータを復号化し、情報表示手段403によって利用者に表示し、終了806へ進む。

【0073】なお、本実施の形態においては可搬型メディアとしてDVD、メディア活用情報の記録領域としてDVD上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやPD、CD-ROMなどの他のメディアや、書換え可能型のDVDを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【0074】また、本実施の形態においては、利用者の秘密鍵をICカードに格納する例について示したが、ICカードへのアクセス時には、ICカード自身に設けられているパスワードなどを別途用いて、利用者以外の第三者からのアクセスを排除することも可能である。さらに、利用者の秘密鍵はICカードに格納するのではなく、DVD再生装置自身の記憶領域に暗号化して記録しておき、利用者のパスワード入力などによって復号化して利用するといった形態や、磁気カードに記録しておくといった形態、利用者自身が覚えておいて、都度入力するといった形態も可能である。

【0075】また、本実施の形態においては特に述べなかったが、映画作品DVDの中に複数の映画作品が記録されている場合に、データ暗号化鍵を映画作品ごとに設けることも可能である。その場合には、DVD情報のエントリとしては、タイトル情報とともにDVD内の映画作品を区別する情報でデータ暗号化鍵を管理し、DVD再生装置からデータ暗号化鍵の取得を依頼する場合にも、DVD内の映画作品を区別する情報をともに鍵管理サーバに送信することになる。

【0076】また、本実施の形態においては、利用者を一人であると仮定していたが、家族など、複数の利用者が映画作品DVDを利用するということがあらかじめ分かっている場合には、複数の利用者それぞれの公開鍵を利用者情報として管理し、複数の発行番号情報を一枚の映画作品DVDに設けることで、利用者を特定したり、あるいは、一つの発行番号情報に対して一定の個数まで利用者を設定できるようにして、何番目の利用者である

かという情報をもとに利用者を特定したりといった方法で、利用者公開鍵を取得するようにし、それぞれの利用者による映画作品DVDの利用を可能とすることができる。

【0077】また、本実施の形態においては特に述べなかったが、データ暗号化鍵・利用者の秘密鍵の漏洩を防止するために、ICカード駆動手段410、データ暗号化鍵復号化手段411は、情報表示手段403を実現するハードウェアに組み込むことによって実装してもよい。

【0078】また、本実施の形態においては特に述べなかったが、鍵管理サーバ自身の認証を行なうために、鍵管理サーバの秘密鍵を用いた公開鍵暗号方式における署名を前記(数1)で示されるデータに施し、ともにDVD再生装置に送信し、DVD再生装置では、鍵管理サーバの公開鍵を用いることで、鍵管理サーバの署名を認証したのち、前記(数4)と前記(数5)に示す方法でデータ暗号化鍵を取得するといった形態も可能である。

【0079】また、本実施の形態では、その時限りの疑似変化を与えることのできる疑似変化情報として乱数を用いたが、これに限ったわけではなく、クレジットカード番号などを暗号化した場合に、クレジットカード自身は解読できないにしても、暗号化した結果が一定とならないように、更にその時限りの疑似変化を与えられるものならば一向に構わない。

【0080】以上のように、本実施の形態では、可搬型メディアを利用できるのは、タイトル情報ごとの発行番号情報に対して、利用者の保持する秘密鍵と一対の公開鍵を登録済みの特定された利用者であって、かつ、利用の際には利用者ごとの秘密鍵を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止するとともに悪意の利用者のなりすましを防止できる。

【0081】また、サーバ認証のステップがないためシステム構成が簡単になるとともに悪意のサーバのなりすましに対してもタイトル情報と発行番号情報が漏洩するのみで済む。

【0082】更に、メディア活用情報は、可搬型メディアの金型でプレスするものではないため、大量に同一の内容を持つ可搬型メディアをプレスしたあとに、一枚ごとにメディア活用情報を記録することで、暗号化データのプレスのためには共通の金型を用いることができるというコスト低下など、その実用的効果は大きい。

【0083】(実施の形態3) 次に、請求項6及び7に対応する第3の実施の形態について説明する。図9は、本実施の形態による、可搬型メディアとして映画作品を記録した、視聴の都度対価の支払いを行なう映画作品再生システムの構成を示す図である。

【0084】また、料金の支払はクレジットカードにより行い、視聴の都度、料金サーバに視聴料金を問合せた上でクレジットカード番号を通知することにより、クレジットカード番号を総務する。なお、クレジットカード番号は、視聴の都度料金サーバに対して通知するものとする。

【0085】図9において、900はDVD再生装置である。901は前記DVD再生装置900の動作全体を制御する中央制御手段、902は前記DVD再生装置900に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、903は利用者に対して前記DVD再生装置900が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、904は前記DVD再生装置900のネットワークに対する情報の送受信を行なう情報送受信手段、905は前記情報送受信手段904などから得られる情報を一時的に記憶しておく情報記憶手段である。906は映画作品をデータ暗号化鍵Dで暗号化して記録した映画作品DVDであって、そのメディア活用情報記録領域には、映画作品DVDの種類を特定可能なタイトル情報と、料金サーバの、公開鍵暗号方式における公開鍵が記録されている。907は前記映画作品DVD906を駆動するDVD駆動手段である。912はクレジットカード番号を料金サーバに送信する際に、クレジットカード番号を、料金サーバの公開鍵を用いて暗号化し、暗号化クレジットカード番号とする、送信データ暗号化手段である。

【0086】920は映画作品DVD906に記録されている映画作品の視聴料金を徴収する料金サーバである。921は前記料金サーバ20の動作全体を制御する中央制御手段、924は前記料金サーバ920のネットワークに対する情報の送受信を行なう情報送受信手段、925は前記情報送受信手段924などから得られる情報や、料金サーバ920自身で生成した情報を一時的に記憶しておく情報記憶手段である。929は公開鍵暗号方式における、前記料金サーバの公開鍵に対応する料金サーバの秘密鍵が記録されているICカード、930は前記ICカード929を駆動するICカード駆動手段である。931は前記料金サーバの秘密鍵を用いて、前記暗号化クレジットカード番号を復号化して、クレジットカード番号を生成する受信データ復号化手段である。933は前記送信データ暗号化手段912において利用する乱数を発生させる乱数発生手段、935は映画作品DVDを再生する場合に請求される料金を前記タイトル情報によって管理するDVD情報管理手段である。940は前記DVD再生装置900と前記料金サーバ920との間を繋ぐネットワークである。950は前記料金サーバ920以外の、他の料金サーバ群、951は前記料金サーバ群950に属する複数の料金サーバと前記料金サーバ920とを合わせた全体を示している。

【0087】図10は、本実施の形態にかかわるメディア活用情報の構成例である。図10において、1000はメディア活用情報、メディア活用情報1000のうち、1001は映画作品DVDの種類を特定可能なタイトル情報、1004は料金サーバの、公開鍵暗号方式における公開鍵と、料金サーバ自身を特定する情報として、電話番号やネットワークアドレスを含む、料金サーバ公開鍵情報であり、映画作品DVD配布時には既に前記メディア活用情報記録領域に記録済みである。

【0088】図11は、本実施の形態にかかわるDVD情報の構成例である。図11において、1100はDVD情報、1101は前記メディア活用情報1000内に含まれるタイトル情報、1103はこのタイトル情報1101によって特定可能な種類の映画作品DVDを再生する場合に請求される料金を含む料金情報である。なお、ここでは、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記DVD情報管理手段935によって管理されている。

【0089】図12は本実施の形態の処理の流れを示すフローチャートである。以下、図9から図12を用いて本発明の第3の実施の形態の動作を説明する。利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品DVD906を入手する。以降、利用者が映画作品DVDを再生する場合の、クレジットカード番号の送信処理について、図12のフローチャートに沿って説明する。なお、図12においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、矢印は処理の流れを示している。

【0090】まず、利用者は、映画作品DVD906をDVD再生装置900のDVD駆動手段907にセットし、入力手段902を用いて、再生開始をDVD再生装置900の中央制御手段901に指示する。これにより、開始1200に示すように、まず、料金支払いのためのクレジットカード番号の送信が開始される。

【0091】次に、ステップ1201に示すように、DVD再生装置900の中央制御手段901はクレジットカード番号送信の指示を受け付け、DVD駆動手段907によって映画作品DVD906のメディア活用情報1000のうち、タイトル情報1001と料金サーバ公開鍵情報1004とを得て、料金サーバ公開鍵情報1004から料金サーバを特定し、タイトル情報1001を、情報送受信手段904により、ネットワーク940を経由して、特定された料金サーバに対して送信し、まず乱数と料金情報との取得を依頼し、ステップ1202に進む。ここで、特定される料金サーバは、説明の便宜上、料金サーバ群951のうちの920であるとし、以下の説明を続ける。

【0092】次に、ステップ1202に示すように、料

金サーバ920の中央制御手段921は、乱数と料金情報との取得依頼の指示を、情報送受信手段924によりタイトル情報1001とともに受信し、乱数発生手段933により乱数Rを発生させ、情報記憶手段925に乱数Rを記憶させ、DVD情報管理手段によりタイトル情報1001から料金情報1103を得て、乱数Rと料金情報1103とを、情報送受信手段924により、ネットワーク940を経由して、DVD再生装置900に送信し、ステップ1203に進む。ここで、メディア活用情報1000内のタイトル情報1001とDVD情報1100内のタイトル情報1101とは等しいものである。

【0093】次に、ステップ1203に示すように、DVD再生装置900の中央制御手段901は、乱数Rと料金情報1103とを情報送受信手段904により受信し、乱数Rは情報記憶手段905に記憶させ、料金情報1103は情報表示手段903に表示させたのち、入力手段902を利用して、利用者にクレジットカード番号Nを入力させ、ステップ1204に進む。

【0094】次に、ステップ1204に示すように、送信データ暗号化手段912は、情報記憶手段905に記憶させておいた乱数Rと、DVD駆動手段907によって映画作品DVD906のメディア活用情報1000から得られる料金サーバ公開鍵情報1004に含まれている料金サーバ公開鍵PSとを用いて、ステップ1203において利用者が入力したクレジットカード番号Nを暗号化し、ステップ1205に進む。ここで、ここで、乱数Rと料金サーバ公開鍵PSによる暗号化の関数を、それぞれe1、e2として、暗号化の様子を模式的に表すと、暗号化されたデータは次の(数6)のようになる。e1、e2の引数は、それぞれ、一つ目の引数が暗号化鍵、二つ目の引数が暗号化されるデータである。

【0095】

【数6】 $e2(PS, R + e1(R, N))$

次に、ステップ1205に示すように、DVD再生装置900の中央制御手段901の指示により、情報送受信手段904により、ネットワーク940を経由して、料金サーバ920に対して、(数6)で示される、暗号化されたクレジットカード番号を送信する。

【0096】次に、ステップ1206に示すように、料金サーバ920は情報送受信手段924によりDVD再生装置900からの(数6)で示されるデータを受信し、さらに、中央制御手段921の指示に従い、ICカード駆動手段930は、ICカード929に格納されている料金サーバ秘密鍵SSを得て、受信データ復号化手段931により、得られたデータ内の乱数Rが情報記憶手段925に記憶してある乱数と等しいことを確認した上で、クレジットカード番号Nを得て、終了1207に進む。ここで、乱数Rと料金サーバ秘密鍵SSによる復号化の関数を、それぞれd1、d2として、復号化の関

子を模式的に表すと、受信データ復号化手段の動作は以下の(数9)から(数10)のように表される。d1、d2の引数は、それぞれ、一つ目の引数が暗号化鍵、二つ目の引数が復号化されるデータであり、前記暗号化の関数e1、e2とは、逆の関係にあり、それぞれ(数7)と(数8)に示すような関係がある。この式に現れるX、Yは暗号化される対象のデータを示す変数である。(数9)と(数10)との操作の間には、(数9)において得られる値R'が、情報記憶手段925に記憶してある乱数Rと等しいかどうかの確認を行なう。

【0097】

【数7】 $d1(R, e1(R, X)) = X$

【0098】

【数8】 $d2(SS, e2(PS, Y)) = Y$

【0099】

【数9】 $d2(SS, e2(PS, R' + e1(R', N))) = R' + e1(R', N)$

【0100】

【数10】 $d1(R, e1(R, N)) = N$

なお、本実施の形態においては可搬型メディアとしてDVD、メディア活用情報の記録領域としてDVD上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやPD、CD-ROMなどの他のメディアや、書換え可能型のDVDを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【0101】また、本実施の形態においては、料金サーバの秘密鍵をICカードに格納する例について示したが、ICカードへのアクセス時には、ICカードに設けられているパスワードなどを別途用いて、料金サーバ管理者以外の第三者からのアクセスを排除することも可能である。さらに、料金サーバの秘密鍵はICカードに格納するのではなく、料金サーバ自身の記憶領域に暗号化して記録しておき、料金サーバ管理者のパスワード入力などによって復号化して利用するといった形態や、磁気カードに記録しておくといった形態、料金サーバ管理者自身が覚えておいて、都度入力するといった形態も可能である。

【0102】また、本実施の形態においては特に述べなかったが、映画作品DVDの中に複数の映画作品が記録されている場合に、料金情報を映画作品ごとに設けることも可能である。その場合には、DVD情報のエントリとしては、タイトル情報とともにDVD内の映画作品を区別する情報で料金情報を管理し、DVD再生装置から乱数と料金情報の取得を依頼する場合にも、DVD内の映画作品を区別する情報をともに鍵管理サーバに送信することになる。

【0103】また、本実施の形態においては特に述べなかったが、利用者自身の認証を行なうために、利用者の秘密鍵を用いた公開鍵暗号方式における署名を前記(数

6)で示されるデータに施し、ともに料金サーバに送信し、料金サーバでは、利用者の公開鍵を用いることで、利用者の署名を認証したのち、前記(数4)と前記(数5)に示す方法でクレジットカード番号を取得するといった形態も可能である。

【0104】また、本実施の形態においては特に述べなかったが、クレジットカード番号を、映画作品DVDの利用の都度、利用者に入力させるのではなく、暗号化してDVD再生装置に記憶させておき、パスワードを入力することでクレジットカード番号を送信するといった形態も可能である。

【0105】また、本実施の形態においては特に述べなかったが、クレジットカード番号を入力する前に、情報表示手段において表示される料金情報を見て、映画作品DVDの再生を実行するかどうかを判断し、その結果、再生を取り止める場合には、クレジットカード番号の送信も中止するといった形態も考えられる。

【0106】また、本実施の形態においてはメディア活用情報記録領域に記録されている料金サーバ公開鍵情報は一つであって、可搬型メディアごとに異なりうる構成としたが、複数の料金サーバ、あるいは全部の料金サーバの公開鍵情報をあらかじめメディア活用情報記録領域に記録しておくという形態も考えられる。この場合、選択する料金サーバによって異なる料金を徴収したり、一時的に料金を下げたりといった使い方も考えられる。

【0107】以上のように、本実施の形態では、利用者から料金サーバに安全にデータを送信する際に必要とする、料金サーバの公開鍵の取得が容易であり、かつ、料金サーバの公開鍵が可搬型メディアごとに異なるものであっても良い。

【0108】また、同一タイトルを含む可搬型メディアであっても公開鍵を異なるものであっても良いため、複数の料金サーバを設けることが可能で、その実用的効果は大きい。

【0109】(実施の形態4)次に、請求項8、9及び10に対応する第4の実施の形態について説明する。図13は、本発明の第4の実施の形態による、可搬型メディアとして映画作品を記録した、視聴の都度、視聴のための可搬型メディアの使用量の記録を行なう映画作品再生システムの構成を示す図である。

【0110】図13において、1300はDVD再生装置である。1301は前記DVD再生装置1300の動作全体を制御する中央制御手段、1302は前記DVD再生装置1300に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、1303は利用者に対して前記DVD再生装置1300が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、1304は前記DVD再生装置1300のネットワークに対する情報の送受信を行なう情報送受信手段

である。1306は映画作品を記録した映画作品DVDであって、そのメディア活用情報記録領域には、映画作品DVDの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報が記録されている。1307は前記映画作品DVD1306を駆動するDVD駆動手段である。

【0111】1320は映画作品DVD1306に記録されている映画作品の視聴のための可搬型メディアの使用量を記録する使用量管理サーバである。1321は前記使用量管理サーバ1320の動作全体を制御する中央制御手段、1324は前記使用量管理サーバ1320のネットワークに対する情報の送受信を行なう情報送受信手段、1334は映画作品DVDを再生する場合の可搬型メディアの使用量を前記タイトル情報と前記発行番号情報とによって管理する利用者情報管理手段である。1340は前記DVD再生装置1300と前記使用量管理サーバ1320との間を繋ぐネットワークである。

【0112】図14は、本実施の形態にかかわるメディア活用情報の構成例である。図14において、1400はメディア活用情報、メディア活用情報1400のうち、1401は映画作品DVDの種類を特定可能なタイトル情報、1402は該映画作品DVDを他のものと識別可能な、前記タイトル情報ごとの発行番号情報であり、映画作品DVD配布時には既に前記メディア活用情報記録領域に記録済みである。

【0113】図15は、本実施の形態にかかわる利用者情報の構成例である。図15において、1500は利用者情報、1501は前記メディア活用情報1400内に含まれるタイトル情報、1502は前記メディア活用情報1400内に含まれる発行番号情報、1504は前記タイトル情報1501と前記発行番号情報1502によって特定可能な可搬型メディアの使用量の累計を示す、使用量累計である。なお、ここでは、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段1334によって管理されている。

【0114】図16は本実施の形態の処理の流れを示すフローチャートである。以下、図13から図16を用いて本実施の形態の動作を説明する。利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品DVD1306を入手する。以降、利用者が映画作品DVDを再生する場合の、使用量の管理について、図16のフローチャートに沿って説明する。なお、図16においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【0115】まず、利用者は、映画作品DVD1306をDVD再生装置1300のDVD駆動手段1307にセットし、入力手段1302を用いて、再生開始をD

D再生装置1300の中央制御手段1301に指示する。これにより、開始1600に示すように、映画作品DVDの再生処理が開始される。

【0116】次に、ステップ1601に示すように、DVD再生装置1300の中央制御手段1301は映画作品DVD1306の再生開始の指示を受け付け、DVD駆動手段1307によって映画作品DVD1306のメディア活用情報1400のうちタイトル情報1401と発行番号情報1402とを得て、タイトル情報1401と発行番号情報1402とを情報送受信手段1304により、ネットワーク1340を経由して、使用量管理サーバ1320に対して送信し、ステップ1602に進む。次に、ステップ1602に示すように、使用量管理サーバ1320の中央制御手段1321は、情報送受信手段1324によりタイトル情報1401と発行番号情報1402とを受信し、利用者情報管理手段1334に対して、タイトル情報1401と発行番号情報1402とで管理されている利用者情報の使用量累計を加算するように指示し、判断1603に進む。

【0117】次に、判断1603に示すように、利用者情報管理手段1334は、利用者情報を参照し、タイトル情報1401で発行番号情報1402の利用者情報のエントリが既に登録されているかどうかを判断する。ここで、利用者情報1500として登録されている場合にはステップ1605に進み、登録されていない場合には、ステップ1604に進む。

【0118】ステップ1604では、利用者情報管理手段1334はタイトル情報1401で発行番号情報1402の利用者情報のエントリを新たに作成して登録し、ステップ1605に進む。説明の便宜上、この新しいエントリを以降1500とする。

【0119】次に、ステップ1605に示すように、利用者情報管理手段1334は、利用者情報1500の使用量累計1504に対して、新たに今回の使用量を加算し、加算された結果の使用量累計1504を情報送受信手段1324により、ネットワーク1340を経由して、DVD再生装置1300に送信し、ステップ1606に進む。

【0120】次に、ステップ1606に示すように、DVD再生装置1300の中央制御手段1301は、使用量累計1504を情報送受信手段1304により受信し、情報表示手段1303にこれを表示したうえで、映画作品DVD1306の再生を開始し、終了1607に進む。

【0121】なお、本実施の形態においては可搬型メディアとしてDVD、メディア活用情報の記録領域としてDVD上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやPD、CD-ROMなどの他のメディアや、書き換え可能型のDVDを用い、メディア活用情報の記録領域については、メディア

本体の記録領域を用いることも可能である。

【0122】なお、本実施の形態において、DVDの再生による使用量の算出について詳しく述べなかったが、DVD再生装置1300側で行う場合は、再生されたメディアの使用量を計算する手段を更に設け、再生（該メディアの使用）が終了したら、その使用量を使用量管理サーバ1320へ送信し、新たに使用量累計1504を更新し、一方、使用量管理サーバ1320側で行う場合は、タイトル情報の発行番号の通知を受けた時点で、任意の基準のもと、一定の使用量を加算するなどの方法が考えられる。

【0123】また、請求項10に記載の発明のように、発行番号情報より更に階層的に使用量を管理する場合、つまり、例えば映画作品DVDの中に複数の映画作品が記録されている場合に、使用量累計を映画作品ごとに計算することも可能である。その場合には、利用者情報のエントリとしては、タイトル情報と発行番号情報とともにDVD内の映画作品を区別する情報で使用量累計を管理し、DVD再生装置からDVDの使用を通知する場合にも、DVD内の映画作品を区別する情報をともに使用量管理サーバに送信することになる。図17は、映画作品を区別する情報として映画作品名を用いた場合の利用者情報の構成例である。1700は利用者情報、1701は前記メディア活用情報1400内に含まれるタイトル情報、1702は前記メディア活用情報1400内に含まれる発行番号情報、1707は映画作品名、1704は前記タイトル情報1701と前記発行番号情報1702と前記映画作品名1707とによって特定可能な可搬型メディア内の映画作品の使用量の累計を示す、使用量累計である。ここで、図17においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。

【0124】また、本実施の形態においては特に述べなかったが、使用量累計に加算される量は、タイトル情報、あるいは複数の映画作品が記録されている場合には、映画作品ごとに異なっても良く、その場合には、映画作品DVDを管理するためのDVD情報を設けて、加算すべき使用量を管理しておくという形態も考えられる。

【0125】以上のように、本実施の形態では、可搬型メディアの使用量を管理することにより、使用量に応じた課金を行うことができるとともに、その使用量をもとにユーザの利用状況（市場動向）を分析し、その分析結果を利用してユーザのより細かい要望への対応ができるなど、その実効的効果は大きい。

【0126】（実施の形態5）次に、請求項11又は12に対応する第5の実施の形態について説明する。請求項11に記載の発明のように、第4の実施の形態において、使用量の上限として、最大使用量があらかじめ決められており、利用者情報に記録されている場合には、こ

の最大使用量を超えないかどうかを使用量管理サーバで管理し、超える場合には、その旨をDVD再生装置に通知して、再生できないようにするといった形態も考えられる。これについては、図18に、使用量管理サーバで管理している利用者情報の構成例を示し、図19に、最大使用量による管理を行う場合のフローチャートを示す。

【0127】以下、簡単に図18と図19について説明をする。図18は、前述の形態に対して、更に最大使用量による管理を加えた場合の利用者情報の構成例である。図18において、1800は利用者情報、1801は前記メディア活用情報1400内に含まれるタイトル情報、1802は前記メディア活用情報1400内に含まれる発行番号情報、1804は前記タイトル情報1801と前記発行番号情報1802によって特定可能な可搬型メディアの使用量の累計を示す、使用量累計、1805は、この利用者情報1800に設定されている最大使用量であって、可搬型メディアごとに異なってもよいものである。ここで、図18においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段1334によって管理されている。

【0128】図19は図18と同様、前述の形態に対して、更に最大使用量による管理を加えた場合の処理の流れを示すフローチャートである。図19において、開始1900、ステップ1901はそれぞれ図16で示した開始1600、ステップ1601と同じであるので説明を省略する。

【0129】次に、ステップ1902に示すように、使用量管理サーバ1320の中央制御手段1321は、情報送受信手段1324によりタイトル情報1401と発行番号情報1402とを受信し、利用者情報管理手段1334に対して、タイトル情報1401と発行番号情報1402とで管理されている利用者情報の使用量累計が最大使用量を超えていないかどうかを判断するように指示し、判断1903に進む。

【0130】次に、判断1903に示すように、利用者情報管理手段1334は、利用者情報を参照し、タイトル情報1401で発行番号情報1402の利用者情報のエントリを得て、その使用量累計1804が最大使用量1805を超えているかどうかを判断する。超えていない場合にはステップ1904に進み、超えている場合にはステップ1906に進む。

【0131】ステップ1904に進んだ場合には、利用者情報管理手段1334は、利用者情報1800の使用量累計1804に対して、新たに今回の使用量を加算し、加算された結果の使用量累計1804を情報送受信手段1324により、ネットワーク1340を経由して、DVD再生装置1300に送信し、ステップ1905に示すように、DVD再生装置1300の中央制御手

段1301は、使用量累計1804を情報送受信手段1304により受信し、情報表示手段1303にこれを表示したうえで、映画作品DVD1306の再生を開始し、終了1908に進む。

【0132】一方、ステップ1906に進んだ場合には、使用量管理サーバ1320は、最大使用量を超えていることを情報送受信手段1324により、ネットワーク1340を経由して、DVD再生装置1300に送信し、ステップ1907に示すように、DVD再生装置1300の中央制御手段1301は、最大使用量を超えていることを情報送受信手段1304により受信し、情報表示手段1303にこれを表示し、終了1908に進む。

【0133】次に、請求項12に記載の発明のように、第4の実施の形態において、使用量の上限としての最大使用量がメディア活用情報記録領域に記録されており、初回の利用時に使用量管理サーバに対して、この最大使用量を登録するといった形態も考えられる。これについては、図20に、最大使用量が記録されている場合のメディア活用情報の構成例を示し、図21に、最大使用量を登録する場合のフローチャートを示す。

【0134】以下、簡単に図20と図21について説明をする。図20は、第4の実施の形態において、最大使用量をメディア活用情報にあらかじめ記録しておいた場合の、メディア活用情報の構成例である。図20において、2000はメディア活用情報、メディア活用情報2000のうち、2001は映画作品DVDの種類を特定可能なタイトル情報、2002は該映画作品DVDを他のものと識別可能な、前記タイトル情報ごとの発行番号情報、2005は該映画作品DVDを入手した際に設定されている最大使用量であり、映画作品DVD配布時には既に前記メディア活用情報記録領域に記録済みである。

【0135】図21は第4の実施の形態に対して、最大使用量をメディア活用情報にあらかじめ記録しておいた場合の処理の流れを示すフローチャートである。なお、図21のフローチャートの説明においては、前記図18で示した利用者情報も用いる。開始2100は、図16で示した開始1600と同じであるので説明を省略する。

【0136】次に、ステップ2101に示すように、DVD再生装置1300の中央制御手段1301は映画作品DVD1306の再生開始の指示を受け付け、DVD駆動手段1307によって映画作品DVD1306のメディア活用情報2000のうちタイトル情報2001と発行番号情報2002と最大使用量2005とを得て、タイトル情報2001と発行番号情報2002と最大使用量2005とを情報送受信手段1304により、ネットワーク1340を経由して、使用量管理サーバ1320に対して送信し、ステップ2102に進む。

【0137】次に、ステップ2102に示すように、使用量管理サーバ1320の中央制御手段1321は、情報送受信手段1324によりタイトル情報2001と発行番号情報2002と最大使用量2005とを受信し、利用者情報管理手段1334に対して、タイトル情報2001と発行番号情報2002とで管理されている利用者情報のエントリが既に登録されているかどうかを判断するように指示し、判断2103に進む。

【0138】次に、判断2103に示すように、利用者情報管理手段1334は、利用者情報を参照し、タイトル情報2001で発行番号情報2002の利用者情報のエントリを探し、既に登録されている場合には、利用者情報1800としてステップ2105に進み、登録されていない場合には、ステップ2104に進む。

【0139】ステップ2104に進んだ場合には、利用者情報管理手段1334は、タイトル情報2001で発行番号情報2002の利用者情報1800を新たに作成し、1801としてタイトル情報2001、1802として発行番号情報2002、1805として最大使用量2005を設定し、ステップ2105に進む。

【0140】次に、ステップ2105に示すように、利用者情報管理手段1334は、利用者情報1800の使用量累計1804に対して、新たに今回の使用量を加算し、加算された結果の使用量累計1804を情報送受信手段1324により、ネットワーク1340を経由して、DVD再生装置1300に送信し、ステップ2106に進む。

【0141】ステップ2106と終了2107は、それぞれ、図16で示したステップ1606と終了1607と同じであるので説明を省略する。

【0142】以上のように、本実施の形態では、該可搬型メディアの使用量をもとに利用料金を利用者に対して請求したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた最大使用量を超える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止でき、その実用的効果は大きい。

【0143】（実施の形態6）次に、請求項13に対応する第6の実施の形態について説明する。図22は、本実施の形態における、可搬型メディアとして暗号化された映画作品を記録した、視聴の都度、視聴のための可搬型メディアの使用量の記録を行ない、使用量が最大使用量を超えない場合にのみ、鍵管理サーバから、復号用のデータ暗号化鍵を得ることが可能であるような、映画作品再生システムの構成を示す図である。

【0144】図22において、2200はDVD再生装置である。2201は前記DVD再生装置2200の動作全体を制御する中央制御手段、2202は前記DVD再生装置2200に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタ

ン、リモートコントロールボタンなどの入力手段、2203は利用者に対して前記DVD再生装置2200が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、2204は前記DVD再生装置2200のネットワークに対する情報の送受信を行なう情報送受信手段である。2206は映画作品をデータ暗号化鍵Dで暗号化して記録した映画作品DVDであって、そのメディア活用情報記録領域には、映画作品DVDの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報が記録されている。2207は前記映画作品DVD2206を駆動するDVD駆動手段である。2208は前記データ暗号化鍵Dを用いて前記映画作品DVD2206内の暗号化された映画作品を復号化するDVD内データ復号化手段である。2209は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているICカード、2210は前記ICカード2209を駆動するICカード駆動手段である。2211は前記利用者の秘密鍵を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵Dを生成するデータ暗号化鍵復号化手段である。

【0145】2220は映画作品DVD2206に記録されている映画作品の視聴のための可搬型メディアの使用量を記録し、かつ、データ暗号化鍵の管理を行なう鍵管理サーバである。2221は前記鍵管理サーバ2220の動作全体を制御する中央制御手段、2224は前記鍵管理サーバ2220のネットワークに対する情報の送受信を行なう情報送受信手段、2232は利用者に対して送信するデータ暗号化鍵を公開鍵暗号方式における利用者の公開鍵で暗号化する送信データ暗号化手段、2233は前記送信データ暗号化手段2232において利用する乱数を発生させる乱数発生手段、2234は映画作品DVDを再生する場合の可搬型メディアの使用量の累計と、最大使用量と、利用者の公開鍵とを前記タイトル情報と前記発行番号情報とによって管理する利用者情報管理手段、2235は前記データ暗号化鍵を前記タイトル情報によって管理するDVD情報管理手段である。2240は前記DVD再生装置2200と前記鍵管理サーバ2220との間を繋ぐネットワークである。

【0146】図23は、本実施の形態にかかわるメディア活用情報の構成例である。図23において、2300はメディア活用情報、メディア活用情報2300のうち、2301は映画作品DVDの種類を特定可能なタイトル情報、2302は該映画作品DVDを他のものと識別可能な、前記タイトル情報ごとの発行番号情報であり、映画作品DVD配布時には既に前記メディア活用情報記録領域に記録済みである。

【0147】図24は、本実施の形態にかかわる利用者情報の構成例である。図24において、2400は利用者情報、2401は前記メディア活用情報2300内に含まれるタイトル情報、2402は前記メディア活用情

報2300内に含まれる発行番号情報、2403は前記タイトル情報2401と前記発行番号情報2402とで特定可能な映画作品DVDを保有している利用者の、公開鍵暗号方式における公開鍵を含む利用者公開鍵情報、2404は前記タイトル情報2401と前記発行番号情報2402によって特定可能な可搬型メディアの使用量の累計を示す、使用量累計、2405は、この利用者情報2400に設定されている最大使用量であって、可搬型メディアごとに異なっているかもしれないものである。ここで、図24においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段2234によって管理されている。

【0148】図25は、本実施の形態にかかわるDVD情報の構成例である。図25において、2500はDVD情報、2501は前記メディア活用情報2300内にふくまれるタイトル情報、2502はこのタイトル情報2501によって特定可能な種類の映画作品DVD内に記録されている映画作品を暗号化するのに用いたデータ暗号化鍵Dを含むデータ暗号化鍵情報である。ここで、図25においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記DVD情報管理手段2235によって管理されている。

【0149】図26は本実施の形態の処理の流れを示すフローチャートである。以下、図22から図26を用いて本実施の形態の動作を説明する。利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品DVD2206を入手する。

【0150】以降、利用者が映画作品DVDを再生する場合の、使用量の管理と、最大使用量を超えない場合のデータ暗号化鍵の取得を安全に行なう方法について、図26のフローチャートに沿って説明する。なお、図26においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【0151】まず、利用者は、映画作品DVD2206をDVD再生装置2200のDVD駆動手段2207にセットし、入力手段2202を用いて、再生開始をDVD再生装置2200の中央制御手段2201に指示する。これにより、開始2600に示すように、映画作品DVDの再生処理が開始される。

【0152】次に、ステップ2601に示すように、DVD再生装置2200の中央制御手段2201は映画作品DVD2206の再生開始の指示を受け付け、DVD駆動手段2207によって映画作品DVD2206のメディア活用情報2300のうちタイトル情報2301と発行番号情報2302とを得て、タイトル情報2301

と発行番号情報2302とを情報送受信手段2204により、ネットワーク2240を経由して、鍵管理サーバ2220に対して送信し、映画作品DVD2206に記録されているデータの復号化のためのデータ暗号化鍵の取得を依頼し、ステップ2602に進む。

【0153】次に、ステップ2602に示すように、鍵管理サーバ2220の中央制御手段2221は、情報送受信手段2224によりタイトル情報2301と発行番号情報2302とを受信し、利用者情報管理手段2234に対して、タイトル情報2301と発行番号情報2302とで管理されている利用者情報の映画作品DVDの使用量累計が最大使用量を超えているかどうかを判断させる指示を行ない、判断2603に進む。

【0154】次に、判断2603に示すように、利用者情報管理手段2234は、利用者情報を参照し、タイトル情報2301で発行番号情報2302の利用者情報のエントリ2400を得て、その使用量累計2404が最大使用量2405を超えているかどうかを判断する。超えていない場合にはステップ2604に進み、超えている場合にはステップ2610に進む。ここで、利用者情報2400のうちのタイトル情報2401と発行番号情報2402とは、それぞれ前記タイトル情報2301と前記発行番号情報2302とに等しい。

【0155】ここで、ステップ2604に進んだ場合には、利用者情報管理手段2234は、利用者情報2400の使用量累計2404に対して、新たに今回の使用量を加算し、DVD情報管理手段2235において、タイトル情報2301を元に、データ暗号化鍵情報2502を得て、ステップ2605に進む。ここで、DVD情報2500のうちのタイトル情報2501は、前記タイトル情報2301と等しい。

【0156】次に、ステップ2605に示すように、利用者情報管理手段2234によって、タイトル情報2301と発行番号情報2302とを元に、利用者公開鍵情報2403を得て、ステップ2606に進む。

【0157】次に、ステップ2606に示すように、乱数発生手段2233により、乱数Rを発生させ、ステップ2607に進む。

【0158】次に、ステップ2607に示すように、送信データ暗号化手段2232において、前記乱数Rを用いて、前記データ暗号化鍵情報2502に含まれているデータ暗号化鍵Dを暗号化し、さらに、Rと前記暗号化されたDとを組合せたデータを、利用者情報管理手段2234によって得られる利用者公開鍵情報2403に含まれている利用者公開鍵PUによって暗号化し、その結果を、情報送受信手段2224により、ネットワーク2240を経由してDVD再生装置2200に送信し、ステップ2608に進む。

【0159】次に、ステップ2608に示すように、DVD再生装置2200は情報送受信手段2204により

鍵管理サーバ2220からの暗号化されたデータを受信し、さらに、中央制御手段2201の指示に従い、ICカード駆動手段2210は、ICカード2209に格納されている利用者秘密鍵S_Uを得て、データ暗号化鍵復号化手段2211により、データ暗号化鍵Dを得て、ステップ2609に進む。

【0160】次に、ステップ2609に示すように、DVD内データ復号化手段2208はステップ2608で得たデータ暗号化鍵Dを用いて、映画作品DVD2206上の暗号化されているデータを復号化し、情報表示手段2203によって利用者に表示し、終了2612へ進む。

【0161】一方、判断2603からステップ2610に進んだ場合には、鍵管理サーバ2220は、最大使用量を超えていることを情報送受信手段2224により、ネットワーク2240を経由して、DVD再生装置2200に送信し、ステップ2611に進む。

【0162】次に、ステップ2611に示すように、DVD再生装置2200の中央制御手段2201は、最大使用量を超えていることを情報送受信手段2204により受信し、情報表示手段2203にこれを表示し、終了2612へ進む。

【0163】なお、本実施の形態においては可搬型メディアとしてDVD、メディア活用情報の記録領域としてDVD上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやPD、CD-ROMなどの他のメディアや、書換え可能型のDVDを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【0164】以上のように、本実施の形態では、該可搬型メディアの使用量を記録することが可能であるため、あらかじめ利用者から徴収した料金に見合う最大使用量を設定しておき、使用量累計が最大使用量に達するまでは利用者の要求に応じてデータ暗号化鍵を渡して、可搬型メディアの使用の可否を制御することにより、可搬型メディアの無制限な利用を確実に防止でき、その実用効果は大きい。

【0165】（実施の形態7）次に、請求項13に記載の発明に請求項14に記載の発明を結合させた第7の実施の形態について説明する。

【0166】図27は、本実施の形態による、可搬型メディアとして暗号化された映画作品を記録した、視聴の都度、視聴のための可搬型メディアの使用量の記録を行ない、使用量が最大使用量を超えない場合にのみ、鍵管理サーバから、復号用のデータ暗号化鍵を得ることが可能であって、かつ、鍵管理サーバに対しては、データを暗号化して送信するような、映画作品再生システムの構成を示す図である。

【0167】図27において、2700はDVD再生装置である。2701は前記DVD再生装置2700の動

作全体を制御する中央制御手段、2702は前記DVD再生装置2700に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、2703は利用者に対して前記DVD再生装置2700が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、2704は前記DVD再生装置2700のネットワークに対する情報の送受信を行なう情報送受信手段、2705は前記情報送受信手段2704などから得られる情報を一時的に記憶しておく情報記憶手段である。2706は映画作品をデータ暗号化鍵Dで暗号化して記録した映画作品DVDであって、そのメディア活用情報記録領域には、映画作品DVDの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報、公開鍵暗号方式における利用者の公開鍵が記録されている。2707は前記映画作品DVD2706を駆動するDVD駆動手段である。2708は前記データ暗号化鍵Dを用いて前記映画作品DVD2706内の暗号化された映画作品を復号化するDVD内データ復号化手段である。2709は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているICカード、2710は前記ICカード2709を駆動するICカード駆動手段である。2711は前記利用者の秘密鍵を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵Dを生成するデータ暗号化鍵復号化手段、2712は鍵管理サーバにデータを送信する際に、鍵管理サーバの公開鍵を用いてデータを暗号化し、暗号化データとする、送信データ暗号化手段である。

【0168】2720は映画作品DVD2706に記録されている映画作品の視聴のための可搬型メディアの使用量を記録し、かつ、データ暗号化鍵の管理を行なう鍵管理サーバである。2721は前記鍵管理サーバ2720の動作全体を制御する中央制御手段、2724は前記鍵管理サーバ2720のネットワークに対する情報の送受信を行なう情報送受信手段、2725は前記情報送受信手段2724から得られる情報や、鍵管理サーバ2720自身で生成した情報を一時的に記憶しておく情報記憶手段である。2729は公開鍵暗号方式における、前記鍵管理サーバの公開鍵に対応する鍵管理サーバの秘密鍵が記録されているICカード、2730は前記ICカード2729を駆動するICカード駆動手段である。2731は前記鍵管理サーバの秘密鍵を用いて、前記DVD再生装置2700から送信されてきた暗号化データを復号化する受信データ復号化手段である。2732は利用者に対して送信するデータ暗号化鍵を公開鍵暗号方式における利用者の公開鍵で暗号化する送信データ暗号化手段、2733は前記送信データ暗号化手段2712と、前記送信データ暗号化手段2732とにおいて利用する乱数を発生させる乱数発生手段、2734は映画作品DVDを再生する場合の可搬型メディアの使用量の累

計と、最大使用量と、利用者の公開鍵とを前記タイトル情報と前記発行番号情報とによって管理する利用者情報管理手段、2735は前記データ暗号化鍵を前記タイトル情報によって管理するDVD情報管理手段である。2740は前記DVD再生装置2700と前記鍵管理サーバ2720との間を繋ぐネットワークである。

【0169】図28は、本実施の形態にかかわるメディア活用情報の構成例である。図28において、2800はメディア活用情報、メディア活用情報2800のうち、2801は映画作品DVDの種類を特定可能なタイトル情報、2802は該映画作品DVDを他のものと識別可能な、前記タイトル情報ごとの発行番号情報、2804は鍵管理サーバの、公開鍵暗号方式における公開鍵を含む、鍵管理サーバ公開鍵情報であり、映画作品DVD配布時には既に前記メディア活用情報記録領域に記録済みである。

【0170】図29は、本実施の形態にかかわる利用者情報の構成例である。図29において、2900は利用者情報、2901は前記メディア活用情報2800内に含まれるタイトル情報、2902は前記メディア活用情報2800内に含まれる発行番号情報、2903は前記タイトル情報2901と前記発行番号情報2902とで特定可能な映画作品DVDを保有している利用者の、公開鍵暗号方式における公開鍵を含む利用者公開鍵情報、2904は前記タイトル情報2901と前記発行番号情報2902によって特定可能な可搬型メディアの使用量の累計を示す、使用量累計、2905は、この利用者情報2900に設定されている最大使用量であって、可搬型メディアごとに異なってもよいものである。ここで、図29においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段2734によって管理されている。

【0171】図30は、本実施の形態にかかわるDVD情報の構成例である。図30において、3000はDVD情報、3001は前記メディア活用情報2800内に含まれるタイトル情報、3002はこのタイトル情報3001によって特定可能な種類の映画作品DVD内に記録されている映画作品を暗号化するのに用いたデータ暗号化鍵Dを含むデータ暗号化鍵情報である。ここで、図30においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記DVD情報管理手段2735によって管理されている。

【0172】図31は、本実施の形態の処理の流れを示すフローチャートである。以下、図27から図31を用いて本実施の形態の動作を説明する。利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品DVD2706を入手する。

【0173】以降、利用者が映画作品DVDを再生する場合の、使用量の管理と、最大使用量を超えない場合のデータ暗号化鍵の取得と取得の以来とを安全に行なう方法について、図31のフローチャートに沿って説明する。なお、図31においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【0174】まず、利用者は、映画作品DVD2706をDVD再生装置2700のDVD駆動手段2707にセットし、入力手段2702を用いて、再生開始をDVD再生装置2700の中央制御手段2701に指示する。これにより、開始3100に示すように、映画作品DVDの再生処理が開始される。

【0175】次に、ステップ3101に示すように、DVD再生装置2700の中央制御手段2701は、情報送受信手段2704により、ネットワーク2740を経由して、鍵管理サーバ2720に対して、まず乱数の取得を依頼し、ステップ3102に進む。

【0176】次に、ステップ3102に示すように、鍵管理サーバ2720の中央制御手段2721は、乱数取得依頼の指示を、情報送受信手段2724により受信し、乱数発生手段2733により乱数Rを発生させ、情報記憶手段2725に乱数Rを記憶させ、乱数Rを、情報送受信手段2724により、ネットワーク2740を経由して、DVD再生装置2700に送信し、ステップ3103に進む。

【0177】次に、ステップ3103に示すように、DVD再生装置2700の中央制御手段2701は、乱数Rを情報送受信手段2704により受信し、乱数Rは情報記憶手段2705に記憶させ、送信データ暗号化手段2712は、情報記憶手段2705に記憶させておいた乱数Rと、DVD駆動手段2707によって映画作品DVD2706のメディア活用情報2800から得られる鍵管理サーバ公開鍵情報2804に含まれている鍵管理サーバ公開鍵PSとを用いて、同じく映画作品DVD2706のメディア活用情報2800から得られるタイトル情報2801と発行番号情報2802とを暗号化し、ステップ3104に進む。

【0178】次に、ステップ3104に示すように、DVD再生装置2700の中央制御手段2701の指示により、情報送受信手段2704は、ネットワーク2740を経由して、鍵管理サーバ2720に対して、暗号化されたタイトル情報2801と発行番号情報2802とを送信し、データ暗号化鍵の取得を鍵管理サーバ2720に依頼し、ステップ3105に進む。

【0179】次に、ステップ3105に示すように、鍵管理サーバ2720は情報送受信手段2724によりDVD再生装置2700からの暗号化されたデータを受信し、さらに、中央制御手段2721の指示に従い、IC

カード駆動手段2730は、ICカード2729に格納されている鍵管理サーバ秘密鍵SSを得て、受信データ復号化手段2731により、タイトル情報2801と発行番号情報2802とを復号化し、判断3106に進む。

【0180】次に、判断3106に示すように、ステップ3105において、送信されたデータから得られた乱数Rが情報記憶手段2725に記憶してある乱数と等しいかどうかを判断し、等しい場合には、Rを用いて正しく復号化できたものとしてステップ3107に進み、等しくない場合には正しく復号化できなかったものとしてステップ3112に進む。

【0181】ステップ3107に進んだ場合には、鍵管理サーバ2720の中央制御手段2721は、ステップ3105で得たタイトル情報2801と発行番号情報2802とを用いて、利用者情報管理手段2734に対して、タイトル情報2801と発行番号情報2802とで管理されている利用者情報の映画作品DVDの使用量累計が最大使用量を超えているかどうかを判断させる指示を行ない、判断3108に進む。

【0182】次に、判断3108に示すように、利用者情報管理手段2734は、利用者情報を参照し、タイトル情報2801で発行番号情報2802の利用者情報のエントリ2900を得て、その使用量累計2904が最大使用量2905を超えているかどうかを判断する。超えていない場合にはステップ3109に進み、超えている場合にはステップ3113に進む。ここで、利用者情報2900のうちのタイトル情報2901と発行番号情報2902とは、それぞれ前記タイトル情報2801と前記発行番号情報2802とに等しい。

【0183】ステップ3109に進んだ場合には、DVD情報管理手段2735は、タイトル情報2801を元に、DVD情報3000からデータ暗号化鍵情報3002を得、利用者情報管理手段2734は、利用者情報2900の使用量累計2904に対して、新たに今回の使用量を加算し、さらに、利用者公開鍵情報2903を得て、ステップ3110に進む。ここで、DVD情報3000のうちのタイトル情報3001は、前記タイトル情報2801と等しい。

【0184】次に、ステップ3110に示すように、送信データ暗号化手段2732において、情報記憶手段2725に記憶してある乱数Rを用いて、前記データ暗号化鍵情報3002に含まれているデータ暗号化鍵Dを暗号化し、さらに、Rと前記暗号化されたDとを組合せたデータを、ステップ3109で得られた利用者公開鍵情報2903に含まれている利用者公開鍵PUによって暗号化し、その結果を、情報送受信手段2724により、ネットワーク2740を経由してDVD再生装置2700に送信し、ステップ3111に進む。

【0185】次に、ステップ3111に示すように、ま

ず、DVD再生装置2700は情報送受信手段2704により鍵管理サーバ2720からの暗号化されたデータを受信し、さらに、中央制御手段2701の指示に従い、ICカード駆動手段2710は、ICカード2709に格納されている利用者秘密鍵SUを得て、データ暗号化鍵復号化手段2711により、データ暗号化鍵Dを得る。この際、情報記憶手段2705に記憶しておいた乱数Rと、データ暗号化鍵復号化手段において得られる乱数とが等しいことを確認する。次に、DVD内データ復号化手段2708において、データ暗号化鍵Dを用いて、映画作品DVD2706上の暗号化されているデータを復号化し、情報表示手段2703によって利用者に表示し、終了3115へ進む。

【0186】また、判断3106からステップ3112に進んだ場合には、ネットワークの障害によってRの値が正しく送信されなかったか、あるいは不正な利用者が介在したために、Rの値が正しく送信されなかったかのどちらかであとし、処理を中断する。

【0187】また、判断3108からステップ3113に進んだ場合には、鍵管理サーバ2720は、最大使用量を超えていることを情報送受信手段2724により、ネットワーク2740を経由して、DVD再生装置2700に送信し、ステップ3114に進む。

【0188】次に、ステップ3114に示すように、DVD再生装置2700の中央制御手段2701は、最大使用量を超えていることを情報送受信手段2704により受信し、情報表示手段2703にこれを表示し、終了3115へ進む。

【0189】なお、本実施の形態においては可搬型メディアとしてDVD、メディア活用情報の記録領域としてDVD上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやPD、CD-ROMなどの他のメディアや、書換え可能型のDVDを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【0190】以上のように、本実施の形態では、該可搬型メディアの使用量を記録することが可能であるため、あらかじめ利用者から徴収した料金に見合う最大使用量を設定しておき、使用量累計が最大使用量に達するまでは利用者の要求に応じてデータ暗号化鍵を渡して、可搬型メディアの使用の可否を制御することにより、可搬型メディアの無制限な利用を確実に防止するという効果を奏するもので、かつ、利用者の要求を鍵管理サーバに送信する場合には、タイトル情報や発行番号情報などの機密の情報が第三者に漏洩することのないように、暗号化して送信することで、安全なデータ転送をも可能とし、その実用的効果は大きい。

【0191】（実施の形態8）次に、請求項15乃至18に対応する第8の実施の形態について説明する。図32は、本発明の第7の実施の形態による、可搬型メデ

アとして映画作品を記録した可搬型メディアに対して、視聴の都度、有効期限を有効期限管理サーバに確認後再生を行なう映画作品再生システムの構成を示す図である。図32において、3200はDVD再生装置である。3201は前記DVD再生装置3200の動作全体を制御する中央制御手段、3202は前記DVD再生装置3200に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、3203は利用者に対して前記DVD再生装置3200が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、3204は前記DVD再生装置3200のネットワークに対する情報の送受信を行なう情報送受信手段である。3206は映画作品を記録した映画作品DVDであって、そのメディア活用情報記録領域には、映画作品DVDの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報とが記録されている。3207は前記映画作品DVD3206を駆動するDVD駆動手段である。

【0192】3220は映画作品DVD3206が使用有効期限内であるかどうかを判断する有効期限管理サーバである。3221は前記有効期限管理サーバ3220の動作全体を制御する中央制御手段、3224は前記有効期限管理サーバ3220のネットワークに対する情報の送受信を行なう情報送受信手段、3234は映画作品DVD使用有効期限を前記タイトル情報と前記発行番号情報とによって管理する利用者情報管理手段、3236は現在時刻を発生させる現在時刻発生手段、3237は現在時刻発生手段3236によって得られた現在時刻と使用有効期限とを比較し、映画作品DVDが使用有効期限内であるかどうかを判断する使用有効期限判断手段である。3240は前記DVD再生装置3200と前記鍵管理サーバ3220との間を繋ぐネットワークである。

【0193】図33は、本実施の形態にかかわるメディア活用情報の構成例である。図33において、3300はメディア活用情報、メディア活用情報3300のうち、3301は映画作品DVDの種類を特定可能なタイトル情報、3302は該映画作品DVDを他のものと識別可能な、前記タイトル情報ごとの発行番号情報であり、映画作品DVD配布時には既に前記メディア活用情報記録領域に記録済みである。

【0194】図34は、本実施の形態にかかわる利用者情報の構成例である。図34において、3400は利用者情報、3401は前記メディア活用情報3300内に含まれるタイトル情報、3402は前記メディア活用情報3300内に含まれる発行番号情報、3406は前記タイトル情報3401と前記発行番号情報3402によって特定可能な可搬型メディアの使用有効期限を示す、使用有効期限情報であって、可搬型メディアごとに異な

っていてもよいものである。ここで、図34においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段3234によって管理されている。

【0195】図35は本実施の形態の処理の流れを示すフローチャートである。以下、図32から図35を用いて本実施の形態の動作を説明する。

【0196】利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品DVD3206を入手する。

【0197】以降、利用者が映画作品DVDを再生する場合の、使用有効期限の管理について、図35のフローチャートに沿って説明する。なお、図35においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【0198】まず、利用者は、映画作品DVD3206をDVD再生装置3200のDVD駆動手段3207にセットし、入力手段3202を用いて、再生開始をDVD再生装置3200の中央制御手段3201に指示する。これにより、開始3500に示すように、映画作品DVD3206の再生処理が開始される。

【0199】次に、ステップ3501に示すように、DVD再生装置3200の中央制御手段3201は映画作品DVD3206の再生開始の指示を受け付け、DVD駆動手段3207によって映画作品DVD3206のメディア活用情報3300のうちタイトル情報3301と発行番号情報3302とを得て、タイトル情報3301と発行番号情報3302とを情報送受信手段3204により、ネットワーク3240を経由して、有効期限管理サーバ3220に対して送信し、ステップ3502に進む。

【0200】次に、ステップ3502に示すように、有効期限管理サーバ3220の中央制御手段3221は、情報送受信手段3224によりタイトル情報3301と発行番号情報3302とを受信し、利用者情報管理手段3234は、これを元に利用者情報3400を得て、そのうちの使用有効期限情報3406を得て、ステップ3503に進む。ここで、3401は前記タイトル情報3301に等しく、3402は前記発行番号情報3302に等しい。

【0201】次に、ステップ3503に示すように、有効期限管理サーバ3220の中央制御手段3221は、現在時刻発生手段3236によって現在時刻Cを発生させ、判断3504に進む。

【0202】次に、判断3504に示すように、使用有効期限判断手段3237において、前記得られた使用有効期限情報3406に含まれている有効期限と現在時刻Cとを比較し、現在時刻Cが有効期限内であるかどうか

を判断し、有効期限内である場合にはステップ3505に進み、有効期間外である場合にはステップ3507に進む。

【0203】ステップ3505に進んだ場合は、有効期限管理サーバ3220の中央制御手段3221は、有効期限内である旨を情報送受信手段3224により、ネットワーク3240を経由して、DVD再生装置3200に送信し、ステップ3506に進む。

【0204】次に、ステップ3506に示すように、DVD再生装置3200の中央制御手段3201は、有効期限内である旨を情報送受信手段3204により受信し、情報表示手段3203にこれを表示したうえで、映画作品DVD3206の再生を開始し、終了3509に進む。

【0205】また、ステップ3507に進んだ場合は、有効期限管理サーバ3220の中央制御手段3221は、有効期限外である旨を情報送受信手段3224により、ネットワーク3240を経由して、DVD再生装置3200に送信し、ステップ3508に進む。

【0206】次に、ステップ3508に示すように、DVD再生装置3200の中央制御手段3201は、有効期限外である旨を情報送受信手段3204により受信し、情報表示手段3203にこれを表示し、終了3509に進む。

【0207】また、本実施の形態においては特に述べなかったが、請求項18に記載の発明のように、映画作品DVDの中に更に複数の映画作品が記録されている場合に、使用有効期限を映画作品ごとに設定することも可能である。その場合には、メディア活用情報に、映画作品ごとに使用有効期限情報を設定する形態、あるいは、利用者情報のエントリとして、タイトル情報と発行番号情報とともにDVD内の映画作品を区別する情報で使用有効期限を管理し、DVD再生装置からDVDの使用を通知する場合にも、DVD内の映画作品を区別する情報とともに使用量管理サーバに送信することになる。

【0208】図39は、映画作品を区別する情報として映画作品名を用いた場合の利用者情報の構成例である。3900は利用者情報、3901は前記メディア活用情報3300内に含まれるタイトル情報、3902は前記メディア活用情報3300内に含まれる発行番号情報、3907は映画作品名、3906は前記タイトル情報3901と前記発行番号情報3902と前記映画作品名3907とによって特定可能な可搬型メディア内の映画作品の使用有効期限を示す、使用有効期限情報である。ここで、図39においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。

【0209】このように、本実施の形態では、可搬型メディアに対してあらかじめ使用有効期限を設定した場合に、それを越えて該可搬型メディアを利用しようとする

場合にその旨通知したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた利用期間を超える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止するという効果を奏するものである。

【0210】（実施の形態9）次に、請求項19乃至22に対応する第9の実施の形態について説明する。本実施の形態は、第8の実施の形態と異なる点として、使用有効期限情報を有効期限管理サーバではなく、可搬型メディアのメディア活用情報にあらかじめ記録しておき、可搬型メディアの利用の都度、メディア活用情報内の使用有効期限情報を有効期限管理サーバに対して送信し、有効期限内であるかどうかの判断をさせるといった形態にある。図36は、この場合の構成例を示したものであり、利用者情報管理手段がない点を除けば、図32の構成と同じ構成である。

【0211】図37は、この場合のメディア活用情報の構成例であって、3700はメディア活用情報、メディア活用情報3700のうち、3706は該映画作品DVDの使用有効期限を示した使用有効期限情報であり、映画作品DVD配布時には既に前記メディア活用情報記録領域に記録済みである。

【0212】図38は、この場合の処理の流れを示すフローチャートであり、図35のフローチャートとの相違は、ステップ3801に示すように、DVD再生装置3600の中央制御手段3601が映画作品DVD3606の再生開始の指示を受け付けた際に、DVD駆動手段3607によって映画作品DVD3606のメディア活用情報3700のうち使用有効期限情報3706を得て、使用有効期限情報3706を情報送受信手段3604により、ネットワーク3640を経由して、有効期限管理サーバ3620に対して送信し、ステップ3802に進む点。

【0213】次に、ステップ3802に示すように、有効期限管理サーバ3620の中央制御手段3621は、情報送受信手段3624により使用有効期限情報3706を受信し、そこから有効期限を得る点であり、その後の、有効期限を使用有効期限判断手段における現在時刻との比較を行い、その結果をDVD再生装置3600に送信し、終了するまでのステップ3803から終了3809までの動作は図35のフローチャートに記載したステップ3503から終了3509までの動作と同じである。

【0214】また、本実施の形態においては特に述べなかったが、請求項21に記載の発明のように、映画作品DVDの中に更に複数の映画作品が記録されている場合に、使用有効期限を映画作品ごとに設定することも可能である。

【0215】また、本実施の形態においては特に述べなかったが、請求項22に記載の発明のように、可搬型メ

ディアの内容が暗号化されている場合は、使用有効期限内であることが判明した後、実施の形態2と同様の処理を行うことによってメディアの再生が可能となる。

【0216】以上のように、本実施の形態においても、第8の実施の形態と同様の効果が得られることは言うまでもない。

【0217】（実施の形態10）次に、請求項23に対応する第10の実施の形態について説明する。図40は、本実施の形態における、可搬型メディアとして暗号化された映画作品を記録した、視聴の都度、鍵管理サーバに対して使用有効期限の確認を行ない、使用有効期限内である場合にのみ、鍵管理サーバから、復号用のデータ暗号化鍵を得ることが可能であるような、映画作品再生システムの構成を示す図である。

【0218】図40において、4000はDVD再生装置である。4001は前記DVD再生装置4000の動作全体を制御する中央制御手段、4002は前記DVD再生装置4000に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、4003は利用者に対して前記DVD再生装置4000が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、4004は前記DVD再生装置4000のネットワークに対する情報の送受信を行なう情報送受信手段である。4006は映画作品をデータ暗号化鍵Dで暗号化して記録した映画作品DVD、そのメディア活用情報記録領域には、映画作品DVDの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報が記録されている。4007は前記映画作品DVD4006を駆動するDVD駆動手段である。4008は前記データ暗号化鍵Dを用いて前記映画作品DVD4006内の暗号化された映画作品を復号化するDVD内データ復号化手段である。4009は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているICカード、4010は前記ICカード4009を駆動するICカード駆動手段である。4011は前記利用者の秘密鍵を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵Dを生成するデータ暗号化鍵復号化手段である。

【0219】4020は映画作品DVD4006に記録されている映画作品の鍵管理サーバである。4021は前記鍵管理サーバ4020の動作全体を制御する中央制御手段、4024は前記鍵管理サーバ4020のネットワークに対する情報の送受信を行なう情報送受信手段、4032は利用者に対して送信するデータ暗号化鍵を公開鍵暗号方式における利用者の公開鍵で暗号化する送信データ暗号化手段、4033は前記送信データ暗号化手段において利用する乱数を発生させる乱数発生手段、4034は映画作品DVDの使用有効期限情報と利用者の公開鍵とを前記タイトル情報と前記発行番号情報とによ

って管理する利用者情報管理手段、4035は前記データ暗号化鍵を前記タイトル情報によって管理するDVD情報管理手段、4036は現在時刻を発生させる現在時刻発生手段、4037は現在時刻発生手段4036によって得られた現在時刻と使用有効期限とを比較し、映画作品DVDが使用有効期限内であるかどうかを判断する使用有効期限判断手段である。4040は前記DVD再生装置4000と前記鍵管理サーバ4020との間を繋ぐネットワークである。

【0220】図41は、本実施の形態にかかわるメディア活用情報の構成例である。図41において、4100はメディア活用情報、メディア活用情報4100のうち、4101は映画作品DVDの種類を特定可能なタイトル情報、4102は該映画作品DVDを他のものと識別可能な、前記タイトル情報ごとの発行番号情報であり、映画作品DVD配布時には既に前記メディア活用情報記録領域に記録済みである。

【0221】図42は、本実施の形態にかかわる利用者情報の構成例である。図42において、4200は利用者情報、4201は前記メディア活用情報4100内に含まれるタイトル情報、4202は前記メディア活用情報4100内に含まれる発行番号情報、4203は前記タイトル情報4201と前記発行番号情報4202とで特定可能な映画作品DVDを保有している利用者の、公開鍵暗号方式における公開鍵を含む利用者公開鍵情報、4206は前記タイトル情報4201と前記発行番号情報4202によって特定可能な可搬型メディアの使用有効期限を示す、使用有効期限情報であって、可搬型メディアごとに異なってもよいものである。ここで、図42においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段4034によって管理されている。

【0222】図43は、本実施の形態にかかわるDVD情報の構成例である。図43において、4300はDVD情報、4301は前記メディア活用情報4100内にふくまれるタイトル情報、4302はこのタイトル情報4301によって特定可能な種類の映画作品DVD内に記録されている映画作品を暗号化するのに用いたデータ暗号化鍵Dを含むデータ暗号化鍵情報である。ここで、図43においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記DVD情報管理手段4035によって管理されている。

【0223】図44は本実施の形態の処理の流れを示すフローチャートである。以下、図40から図44を用いて本実施の形態の動作を説明する。利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品DVD4006を入手する。

【0224】以降、利用者が映画作品DVDを再生する場合の、使用有効期限の管理と、使用有効期限を超えない場合のデータ暗号化鍵の取得を安全に行なう方法について、図44のフローチャートに沿って説明する。なお、図44においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【0225】まず、利用者は、映画作品DVD4006をDVD再生装置4000のDVD駆動手段4007にセットし、入力手段4002を用いて、再生開始をDVD再生装置4000の中央制御手段4001に指示する。これにより、開始4400に示すように、映画作品DVD4006の再生処理が開始される。

【0226】次に、ステップ4401に示すように、DVD再生装置4000の中央制御手段4001は映画作品DVD4006の再生開始の指示を受け付け、DVD駆動手段4007によって映画作品DVD4006のメディア活用情報4100のうちタイトル情報4101と発行番号情報4102とを得て、タイトル情報4101と発行番号情報4102とを情報送受信手段4004により、ネットワーク4040を経由して、鍵管理サーバ4020に対して送信し、映画作品DVD4006に記録されているデータの復号化のためのデータ暗号化鍵の取得を依頼し、ステップ4402に進む。

【0227】次に、ステップ4402に示すように、鍵管理サーバ4020の中央制御手段4021は、情報送受信手段4024によりタイトル情報4101と発行番号情報4102とを受信し、利用者情報管理手段4034に対して、タイトル情報4101と発行番号情報4102とで管理されている利用者情報のエントリ4200を得て、その使用有効期限情報4206を得、また、現在時刻発生手段4036により、現在時刻Cを得て、判断4403に進む。ここで、利用者情報4200のうちのタイトル情報4201と発行番号情報4202とは、それぞれ前記タイトル情報4101と発行番号情報4102とに等しい。

【0228】次に、判断4403に示すように、使用有効期限判断手段4037において、現在時刻Cが、前記得られた使用有効期限情報4206に含まれている有効期限内であるかどうかを判断し、有効期限内である場合には、ステップ4404に進み、有効期限外である場合には、ステップ4410に進む。

【0229】ステップ4404に進んだ場合には、DVD情報管理手段4035は、タイトル情報4101を元に、データ暗号化鍵情報4302を得て、ステップ4405に進む。ここで、DVD情報4300のうちのタイトル情報4301は、前記タイトル情報4101と等しい。

【0230】次に、ステップ4405に示すように、利

用者情報管理手段4034によって、タイトル情報4101と発行番号情報4102とを元に、利用者公開鍵情報4203を得て、ステップ4406に進む。

【0231】次に、ステップ4406に示すように、乱数発生手段4033により、乱数Rを発生させ、ステップ4407に進む。

【0232】次に、ステップ4407に示すように、送信データ暗号化手段4032において、前記乱数Rを用いて、前記データ暗号化鍵情報4302に含まれているデータ暗号化鍵Dを暗号化し、さらに、Rと前記暗号化されたDとを組合せたデータを、利用者情報管理手段4034によって得られる利用者公開鍵情報4203に含まれている利用者公開鍵PUによって暗号化し、その結果を、情報送受信手段4024により、ネットワーク4040を経由してDVD再生装置4000に送信し、ステップ4408に進む。

【0233】次に、ステップ4408に示すように、DVD再生装置4000は情報送受信手段4004により鍵管理サーバ4020からの暗号化されたデータを受信し、さらに、中央制御手段4001の指示に従い、ICカード駆動手段4010は、ICカード4009に格納されている利用者秘密鍵SUを得て、この利用者秘密鍵SUを用いて、データ暗号化鍵復号化手段4011により、データ暗号化鍵Dを得て、ステップ4409に進む。

【0234】次に、ステップ4409に示すように、DVD内データ復号化手段4008は既に得たデータ暗号化鍵Dを用いて、映画作品DVD4006上の暗号化されているデータを復号化し、情報表示手段4003によって利用者に表示し、終了4412へ進む。

【0235】また、判断4403からステップ4410に進んだ場合には、鍵管理サーバ4020は、使用有効期限内ではないことを、情報送受信手段4024により、ネットワーク4040を経由して、DVD再生装置4000に送信し、ステップ4411に進む。

【0236】次に、ステップ4411に示すように、DVD再生装置4000の中央制御手段4001は、使用有効期限内ではないことを、情報送受信手段4004により受信し、情報表示手段4003にこれを表示し、終了4412へ進む。

【0237】なお、本実施の形態においては可搬型メディアとしてDVD、メディア活用情報の記録領域としてDVD上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやPD、CD-R OMなどの他のメディアや、書換え可能型のDVDを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【0238】このように、本実施の形態では、該可搬型メディアの使用有効期限を設定することが可能であるため、あらかじめ利用者から徴収した料金に見合う使用有

効期限を設定しておき、使用有効期限内である間は利用者の要求に応じてデータ暗号化鍵を渡して、可搬型メディアの使用の可否を制御することにより、可搬型メディアの無制限な利用を確実に防止でき、その実用的効果は大きい。

【0239】(実施の形態11)次に、請求項23に記載の発明に請求項24に記載の発明の形態を結合させた第11の実施の形態について説明する。図45は、本実施の形態における、可搬型メディアとして暗号化された映画作品を記録した、視聴の都度、鍵管理サーバに有効期限の確認を行ない、使用有効期限内である場合にのみ、鍵管理サーバから、復号用のデータ暗号化鍵を得ることが可能であるような、映画作品再生システムの構成を示す図である。

【0240】図45において、4500はDVD再生装置である。4501は前記DVD再生装置4500の動作全体を制御する中央制御手段、4502は前記DVD再生装置4500に対して利用者が入力を行なうキーボードやマウス、音声認識装置、タブレット、ペン、ボタン、リモートコントロールボタンなどの入力手段、4503は利用者に対して前記DVD再生装置4500が表示を行なうためのディスプレイ、スピーカなどの情報表示手段、4504は前記DVD再生装置4500のネットワークに対する情報の送受信を行なう情報送受信手段、4505は前記情報送受信手段4504などから得られる情報を一時的に記憶しておく情報記憶手段である。4506は映画作品をデータ暗号化鍵Dで暗号化して記録した映画作品DVDであって、そのメディア活用情報記録領域には、映画作品DVDの種類を特定可能なタイトル情報と、タイトル情報ごとの発行番号情報が記録されている。4507は前記映画作品DVD4506を駆動するDVD駆動手段である。4508は前記データ暗号化鍵Dを用いて前記映画作品DVD4506内の暗号化された映画作品を復号化するDVD内データ復号化手段である。4509は公開鍵暗号方式における、前記利用者の公開鍵に対応する利用者の秘密鍵が記録されているICカード、4510は前記ICカード4509を駆動するICカード駆動手段である。4511は前記利用者の秘密鍵を用いて、前記暗号化データ暗号化鍵を復号化してデータ暗号化鍵Dを生成するデータ暗号化鍵復号化手段、4512は鍵管理サーバにデータを送信する際に、鍵管理サーバの公開鍵を用いてデータを暗号化し、暗号化データとする、送信データ暗号化手段である。

【0241】4520は映画作品DVD4506に記録されている映画作品の鍵管理サーバである。4521は前記鍵管理サーバ4520の動作全体を制御する中央制御手段、4524は前記鍵管理サーバ4520のネットワークに対する情報の送受信を行なう情報送受信手段、4525は前記情報送受信手段4524などから得られ

る情報や、鍵管理サーバ4520自身で生成した情報を一時的に記憶しておく情報記憶手段である。4529は公開鍵暗号方式における、前記鍵管理サーバの公開鍵に対応する鍵管理サーバの秘密鍵が記録されているICカード、4530は前記ICカード4529を駆動するICカード駆動手段である。4531は前記鍵管理サーバの秘密鍵を用いて、前記DVD再生装置4500から送信されてきた暗号化データを復号化する受信データ復号化手段である。4532は利用者に対して送信するデータ暗号化鍵を公開鍵暗号方式における利用者の公開鍵で暗号化する送信データ暗号化手段、4533は前記送信データ暗号化手段4512と、前記送信データ暗号化手段4532とにおいて利用する乱数を発生させる乱数発生手段、4534は映画作品DVDの使用有効期限情報と利用者の公開鍵とを前記タイトル情報と前記発行番号情報とによって管理する利用者情報管理手段、4535は前記データ暗号化鍵を前記タイトル情報によって管理するDVD情報管理手段、4536は現在時刻を発生させる現在時刻発生手段、4537は現在時刻発生手段4536によって得られた現在時刻と使用有効期限とを比較し、映画作品DVDが使用有効期限内であるかどうかを判断する使用有効期限判断手段である。4540は前記DVD再生装置4500と前記鍵管理サーバ4520との間を繋ぐネットワークである。

【0242】図46は、本実施の形態にかかわるメディア活用情報の構成例である。図46において、4600はメディア活用情報、メディア活用情報4600のうち、4601は映画作品DVDの種類を特定可能なタイトル情報、4602は該映画作品DVDを他のものと識別可能な、前記タイトル情報ごとの発行番号情報、4604は鍵管理サーバの、公開鍵暗号方式における公開鍵を含む、鍵管理サーバ公開鍵情報であり、映画作品DVD配布時には既に前記メディア活用情報記録領域に記録済みである。

【0243】図47は、本実施の形態にかかわる利用者情報の構成例である。図47において、4700は利用者情報、4701は前記メディア活用情報4600内に含まれるタイトル情報、4702は前記メディア活用情報4600内に含まれる発行番号情報、4703は前記タイトル情報4701と前記発行番号情報4702とで特定可能な映画作品DVDを保有している利用者の、公開鍵暗号方式における公開鍵を含む利用者公開鍵情報、4706は前記タイトル情報4701と前記発行番号情報4702によって特定可能な可搬型メディアの使用有効期限を示す、使用有効期限情報であって、可搬型メディアごとに異なってもよいものである。ここで、図47においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記利用者情報管理手段4534によって管理されている。

【0244】図48は、本実施の形態にかかわるDVD情報の構成例である。図48において、4800はDVD情報、4801は前記メディア活用情報4600内に含まれるタイトル情報、4802はこのタイトル情報4801によって特定可能な種類の映画作品DVD内に記録されている映画作品を暗号化するのに用いたデータ暗号化鍵Dを含むデータ暗号化鍵情報である。ここで、図48においては、一つのエントリのみ示したが、実際には、このような形式で複数のエントリが存在する。これらは前記DVD情報管理手段4535によって管理されている。

【0245】図49は、本実施の形態の処理の流れを示すフローチャートである。以下、図45から図49を用いて本実施の形態の動作を説明する。

【0246】利用者は書店や通信販売で購入、あるいは会員制のサービスによって配布してもらうことにより映画作品DVD4506を入手する。

【0247】以降、利用者が映画作品DVDを再生する場合の、使用有効期限の管理と、使用有効期限を超えない場合のデータ暗号化鍵の取得と取得の依頼とを安全に行なう方法について、図49のフローチャートに沿って説明する。なお、図49においては角の丸い長方形で囲われた部分は、フローチャートの開始・終了を示し、長方形で囲われた部分は処理を示し、菱形で囲われた部分は判断を示し、矢印は処理の流れを示している。

【0248】まず、利用者は、映画作品DVD4506をDVD再生装置4500のDVD駆動手段4507にセットし、入力手段4502を用いて、再生開始をDVD再生装置4500の中央制御手段4501に指示する。これにより、開始4900に示すように、映画作品DVDの再生処理が開始される。

【0249】まず、ステップ4901に示すように、DVD再生装置4500の中央制御手段4501は、情報送受信手段4504により、ネットワーク4540を経由して、鍵管理サーバ4520に対して、乱数の取得を依頼し、ステップ4902に進む。

【0250】次に、ステップ4902に示すように、鍵管理サーバ4520の中央制御手段4521は、乱数取得依頼の指示を、情報送受信手段4524により受信し、乱数発生手段4533により乱数Rを発生させ、情報記憶手段4525に乱数Rを記憶させ、乱数Rを、情報送受信手段4524により、ネットワーク4540を経由して、DVD再生装置4500に送信し、ステップ4903に進む。

【0251】次に、ステップ4903に示すように、DVD再生装置4500の中央制御手段4501は、乱数Rを情報送受信手段4504により受信し、乱数Rは情報記憶手段4505に記憶させ、送信データ暗号化手段4512は、乱数Rと、DVD駆動手段4507によって映画作品DVD4506のメディア活用情報4600

から得られる鍵管理サーバ公開鍵情報4604に含まれている鍵管理サーバ公開鍵PSとを用いて、同じく映画作品DVD4506のメディア活用情報4600から得られるタイトル情報4601と発行番号情報4602とを暗号化し、ステップ4904に進む。

【0252】次に、ステップ4904に示すように、DVD再生装置4500の中央制御手段4501の指示により、情報送受信手段4504により、ネットワーク4540を経由して、鍵管理サーバ4520に対して、暗号化されたタイトル情報4601と発行番号情報4602とを送信し、データ暗号化鍵の取得を鍵管理サーバ4520に依頼し、ステップ4905に進む。

【0253】次に、ステップ4905に示すように、鍵管理サーバ4520は情報送受信手段4524によりDVD再生装置4500からの暗号化されたデータを受信し、さらに、中央制御手段4521の指示に従い、ICカード駆動手段4530は、ICカード4529に格納されている鍵管理サーバ秘密鍵SSを得て、受信データ復号化手段4531により、タイトル情報4601と発行番号情報4602とを復号化し、判断4906に進む。

【0254】次に、判断4906に示すように、ステップ4905において、送信されたデータから得られた乱数Rが情報記憶手段4525に記憶してある乱数と等しいかどうかを判断し、等しい場合には、Rを用いて正しく復号化できたものとしてステップ4907に進み、等しくない場合には正しく復号化できなかったものとしてステップ4912に進む。

【0255】ステップ4907に進んだ場合には、鍵管理サーバ4520の中央制御手段4521は、ステップ4905で得たタイトル情報4601と発行番号情報4602とを用いて、利用者情報管理手段4534に対して、タイトル情報4601と発行番号情報4602とで管理されている利用者情報のエントリ4700を得て、その使用有効期限情報4706を得、また、現在時刻発生手段4536により、現在時刻Cを得て、判断4908に進む。ここで、利用者情報4700のうちのタイトル情報4701と発行番号情報4702とは、それぞれ前記タイトル情報4601と前記発行番号情報4602とに等しい。

【0256】次に、判断4908に示すように、使用有効期限判断手段4537において、現在時刻Cが、前記得られた使用有効期限情報4706に含まれている有効期限内であるかどうかを判断し、有効期限内である場合には、ステップ4909に進み、有効期限外である場合には、ステップ4913に進む。

【0257】ステップ4909に進んだ場合には、DVD情報管理手段4535は、タイトル情報4601を元に、DVD情報4800からデータ暗号化鍵情報4802を得、利用者情報管理手段4534は、タイトル情報

4601と発行番号情報4602とを元に、利用者公開鍵情報4703を得て、ステップ4910に進む。ここで、DVD情報4800のうちのタイトル情報4801は、前記タイトル情報4601と等しい。

【0258】次に、ステップ4910に示すように、送信データ暗号化手段4532において、情報記憶手段4525に記憶してある乱数Rを用いて、前記データ暗号化鍵情報4802に含まれているデータ暗号化鍵Dを暗号化し、さらに、Rと前記暗号化されたDとを組合せたデータを、ステップ4909で得られた利用者公開鍵情報4703に含まれている利用者公開鍵PUによって暗号化し、その結果を、情報送受信手段4524により、ネットワーク4540を経由してDVD再生装置4500に送信し、ステップ4911に進む。

【0259】次に、ステップ4911に示すように、DVD再生装置4500は情報送受信手段4504により鍵管理サーバ4520からの暗号化されたデータを受信し、さらに、中央制御手段4501の指示に従い、ICカード駆動手段4510は、ICカード4509に格納されている利用者秘密鍵SUを得て、この利用者秘密鍵SUを用いて、データ暗号化鍵復号化手段4511により、データ暗号化鍵Dを得て、DVD内データ復号化手段4508において、データ暗号化鍵Dを用いて、映画作品DVD4506上の暗号化されているデータを復号化し、情報表示手段4503によって利用者に表示し、終了4915へ進む。

【0260】また、判断4906からステップ4912に進んだ場合には、ネットワークの障害によってRの値が正しく送信されなかったか、あるいは不正な利用者が介在したために、Rの値が正しく送信されなかったかのどちらかであるとし、処理を中断する。

【0261】また、判断4908からステップ4913に進んだ場合には、鍵管理サーバ4520は、使用有効期限内ではないことを、情報送受信手段4524により、ネットワーク4540を経由して、DVD再生装置4500に送信し、ステップ4914に進む。

【0262】次に、ステップ4914に示すように、DVD再生装置4500の中央制御手段4501は、使用有効期限内ではないことを、情報送受信手段4504により受信し、情報表示手段4503にこれを表示し、終了4915へ進む。

【0263】なお、本実施の形態においては可搬型メディアとしてDVD、メディア活用情報の記録領域としてDVD上のメディア活用情報記録領域を用いたが、可搬型メディアとしてフロッピーディスクやPD、CD-ROMなどの他のメディアや、書換え可能型のDVDを用い、メディア活用情報の記録領域については、メディア本体の記録領域を用いることも可能である。

【0264】このように、本実施の形態では、該可搬型メディアの使用有効期限を設定することが可能であるた

め、あらかじめ利用者から徴収した料金に見合う使用有効期限を設定しておき、使用有効期限内である間は利用者の要求に応じてデータ暗号化鍵を渡して、可搬型メディアの使用の可否を制御することにより、可搬型メディアの無制限な利用を確実に防止するという効果を奏するもので、かつ、利用者の要求を鍵管理サーバに送信する場合には、タイトル情報や発行番号情報などの機密の情報が第三者に漏洩することのないように、暗号化して送信することで、安全なデータ転送をも可能にし、その実効効果は大きい。

【0265】

【発明の効果】以上のように本発明によれば、第1に、大容量のデータの記録が可能な可搬型メディア内の暗号化データを復号化するのに必要なデータ暗号化鍵を利用者ごとの秘密情報で解読可能な形式で暗号化して、暗号化データ暗号化鍵とし、この暗号化データ暗号化鍵を、該可搬型メディアそれぞれに固有なメディア活用情報として記録しておき、利用者ごとの秘密情報は別途格納しておくことを特徴とする可搬型メディアの駆動装置であり、可搬型メディア内の暗号化データを復号化する際には、まず利用者ごとの秘密情報を得て、これによって可搬型メディアのメディア活用情報内の暗号化データ暗号化鍵を復号化してデータ暗号化鍵とし、さらにこのデータ暗号化鍵によって可搬型メディア内の暗号化データを復号化する構成としたことにより、可搬型メディアを利用できるのは、あらかじめ特定された利用者であって、かつ、利用の際には利用者ごとの秘密情報を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止できるという効果を奏する。

【0266】第2に、大容量のデータの記録が可能な可搬型メディア内の暗号化データを復号化するのに必要なデータ暗号化鍵を、可搬型メディアのメディア活用情報に記録されているタイトル情報ごとにサーバ側で管理しておき、また、利用者の秘密情報と一対の公開の情報を前記タイトル情報とタイトル情報ごとの発行番号情報ごとにサーバ側で管理しておき、利用者の秘密情報は別途格納しておいてクライアント側で利用することを特徴とする可搬型メディアとネットワークの連携装置であり、利用者はメディア活用情報に記録されているタイトル情報と発行番号情報をサーバ側に通知してデータ暗号化鍵の取得を依頼し、サーバ側は得られたタイトル情報に対応するデータ暗号化鍵を、得られたタイトル情報と発行番号情報に対応する公開の情報と、別途発生させる乱数を用いて暗号化して送り返し、利用者側では利用者ごとの秘密情報を用いて、得られたデータから乱数を分離し、さらにデータ暗号化鍵を得て、暗号化データを復号化して利用する構成としたことにより、可搬型メディア

を利用できるのは、タイトル情報・発行番号情報と、利用者の保持する秘密情報と一対の公開の情報を登録済みの特定された利用者であって、かつ、利用の際には利用者ごとの秘密情報を必要とするため、可搬型メディアを単独では利用することができず、結果として不正な利用を防止し、さらに、メディア活用情報まで含めて不正に複製しても特定された利用者の秘密情報がなければ利用できないため、結果として不正な複製を防止するとともに悪意の利用者のなりすましを防止できるという効果を奏する。

【0267】第3に、可搬型メディアのメディア活用情報にサーバの秘密情報と一対の公開情報を記録しておく、サーバの秘密情報は別途格納しておいてサーバ側で利用することを特徴とする可搬型メディアとネットワークの連携装置であり、利用者からサーバにデータを送信する際には、サーバで別途発生させる乱数と、メディア活用情報内の公開情報を用いて暗号化して送信し、サーバ側では、サーバの秘密情報と前記乱数を用いて得られたデータの正当性を確認したのち、乱数を分離して、利用者からデータを得る構成としたことにより、利用者からサーバに安全にデータを送信する際に必要とする、サーバの公開鍵の取得が容易であるという効果に加え、サーバの公開鍵が可搬型メディアごとに異なるものであっても良いという効果を奏する。

【0268】第4に、可搬型メディアそれぞれに固有のメディア活用情報としてタイトル情報とタイトル情報ごとの発行番号情報を設け、このタイトル情報と発行番号情報とを用いてサーバ側で可搬型メディアの使用量を管理することを特徴とする可搬型メディアとネットワークの連携装置であり、可搬型メディアを利用する際には、メディア活用情報内のタイトル情報と発行番号情報とをサーバに送信し、サーバ側では該可搬型メディアの使用量を加算したり、また、最大使用量が設定されている場合には、それを超えるかどうかの判断を行なう構成としたことにより、該可搬型メディアの使用量をもとに利用料金を利用者に対して請求したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた最大使用量を超える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止するという効果を奏する。

【0269】第5に、前記第2の構成と前記第4の構成とを組合せた可搬型メディアとネットワークの連携装置であり、常にデータ暗号化鍵をサーバから取得するようにし、最大使用量を超える場合にはデータ暗号化鍵を渡さないようにする構成としたことにより、最大使用量を超えての可搬型メディアの無制限な利用を確実に防止するという効果を奏する。

【0270】第6に、前記第3の構成と前記第5の構成とを組合せた可搬型メディアとネットワークの連携装置であり、データ暗号化鍵取得のためのメディア活用情報

を暗号化して送信する構成としたことにより、メディア活用情報に記述されている情報を安全にサーバに送信することが可能であるという効果を奏する。

【0271】第7に、可搬型メディアそれぞれに固有のメディア活用情報として使用有効期限情報を設け、サーバ側には、使用有効期限を判断する手段を設けたことを特徴とする可搬型メディアとネットワークの連携装置、あるいは、可搬型メディアそれぞれに固有のメディア活用情報としてタイトル情報、あるいはタイトル情報とタイトル情報ごとの発行番号情報とを設け、サーバ側には、タイトル情報、あるいはタイトル情報とタイトル情報ごとの発行番号情報とによって該可搬型メディアの使用有効期限を管理する手段と、使用有効期限を判断する手段を設けたことを特徴とする可搬型メディアとネットワークの連携装置であって、可搬型メディアを利用する際には、メディア活用情報内の使用有効期限情報、あるいはタイトル情報、あるいはタイトル情報と発行番号情報とをサーバに送信し、サーバ側で該可搬型メディアが使用可能かどうかを判断することを特徴としたことにより、可搬型メディアに対してあらかじめ使用有効期限を設定した場合に、それを超えて該可搬型を利用しようとする場合にその旨通知したり、また、あらかじめ利用料金を払い込んである場合に、それに応じた利用期間を越える場合にはその旨通知したりといったことが可能であって、可搬型メディアの無制限な利用を防止するという効果が得られる。

【0272】第8に、前記第2の構成と前記第7の構成とを組合せた可搬型メディアとネットワークの連携装置であり、常にデータ暗号化鍵をサーバから取得するようにし、使用有効期限を越える場合にはデータ暗号化鍵を渡さないようにする構成としたことにより、使用有効期限を越えての可搬型メディアの無制限な利用を確実に防止するという効果を奏する。

【0273】第9に、前記第3の構成と前記第8の構成とを組合せた可搬型メディアとネットワークの連携装置であり、データ暗号化鍵取得のためのメディア活用情報を暗号化して送信する構成としたことにより、メディア活用情報に記述されている情報を安全にサーバに送信できるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態における構成例を示す図

【図2】本発明の第1の実施の形態におけるメディア活用情報の構成例を示す図

【図3】本発明の第1の実施の形態における動作のフローチャートを示す図

【図4】本発明の第2の実施の形態における構成例を示す図

【図5】本発明の第2の実施の形態におけるメディア活用情報の構成例を示す図

【図 6】本発明の第 2 の実施の形態における利用者情報の構成例を示す図

【図 7】本発明の第 2 の実施の形態における DVD 情報の構成例を示す図

【図 8】本発明の第 2 の実施の形態における動作のフローチャートを示す図

【図 9】本発明の第 3 の実施の形態における構成例を示す図

【図 10】本発明の第 3 の実施の形態におけるメディア活用情報の構成例を示す図

【図 11】本発明の第 3 の実施の形態における DVD 情報の構成例を示す図

【図 12】本発明の第 3 の実施の形態における動作のフローチャートを示す図

【図 13】本発明の第 4 の実施の形態における構成例を示す図

【図 14】本発明の第 4 の実施の形態におけるメディア活用情報の構成例を示す図

【図 15】本発明の第 4 の実施の形態における利用者情報の構成例を示す図

【図 16】本発明の第 4 の実施の形態における動作のフローチャートを示す図

【図 17】本発明の第 4 の実施の形態における利用者情報の構成の他の例を示す図

【図 18】本発明の第 5 の実施の形態における利用者情報の構成の例を示す図

【図 19】本発明の第 5 の実施の形態における動作のフローチャートを示す図

【図 20】本発明の第 5 の実施の形態におけるメディア活用情報の構成の他の例を示す図

【図 21】本発明の第 5 の実施の形態における他の動作のフローチャートを示す図

【図 22】本発明の第 6 の実施の形態における構成例を示す図

【図 23】本発明の第 6 の実施の形態におけるメディア活用情報の構成例を示す図

【図 24】本発明の第 6 の実施の形態における利用者情報の構成例を示す図

【図 25】本発明の第 6 の実施の形態における DVD 情報の構成例を示す図

【図 26】本発明の第 6 の実施の形態における動作のフローチャートを示す図

【図 27】本発明の第 7 の実施の形態における構成例を示す図

【図 28】本発明の第 7 の実施の形態におけるメディア活用情報の構成例を示す図

【図 29】本発明の第 7 の実施の形態における利用者情報の構成例を示す図

【図 30】本発明の第 7 の実施の形態における DVD 情報の構成例を示す図

【図 31】本発明の第 7 の実施の形態における動作のフローチャートを示す図

【図 32】本発明の第 8 の実施の形態における構成例を示す図

【図 33】本発明の第 8 の実施の形態におけるメディア活用情報の構成例を示す図

【図 34】本発明の第 8 の実施の形態における利用者情報の構成例を示す図

【図 35】本発明の第 8 の実施の形態における動作のフローチャートを示す図

【図 36】本発明の第 9 の実施の形態における構成の例を示す図

【図 37】本発明の第 9 の実施の形態におけるメディア活用情報の構成の例を示す図

【図 38】本発明の第 9 の実施の形態における動作のフローチャートを示す図

【図 39】本発明の第 8 の実施の形態における利用者情報の構成の他の例を示す図

【図 40】本発明の第 10 の実施の形態における構成例を示す図

【図 41】本発明の第 10 の実施の形態におけるメディア活用情報の構成例を示す図

【図 42】本発明の第 10 の実施の形態における利用者情報の構成例を示す図

【図 43】本発明の第 10 の実施の形態における DVD 情報の構成例を示す図

【図 44】本発明の第 10 の実施の形態における動作のフローチャートを示す図

【図 45】本発明の第 11 の実施の形態における構成例を示す図

【図 46】本発明の第 11 の実施の形態におけるメディア活用情報の構成例を示す図

【図 47】本発明の第 11 の実施の形態における利用者情報の構成例を示す図

【図 48】本発明の第 11 の実施の形態における DVD 情報の構成例を示す図

【図 49】本発明の第 11 の実施の形態における動作のフローチャートを示す図

【符号の説明】

200 メディア活用情報

203 データ暗号化鍵情報

501 タイトル情報

502 発行番号情報

600 利用者情報

603 利用者公開鍵情報

700 DVD 情報

1000 料金サーバ公開情報

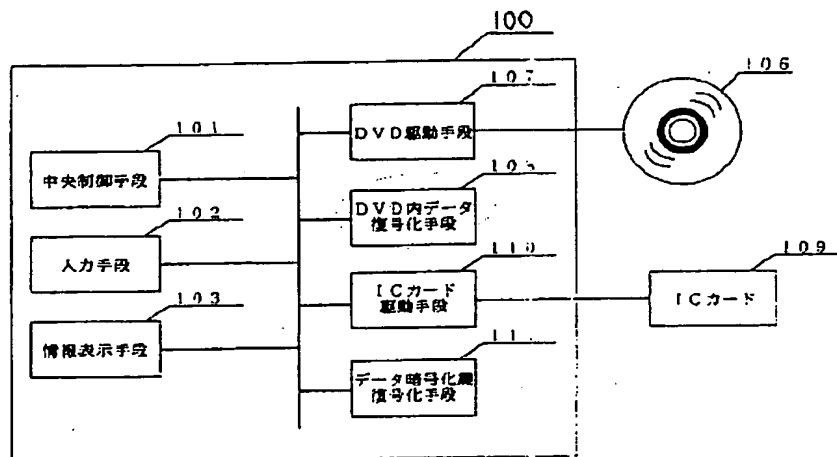
1103 料金情報

1504 使用量累計

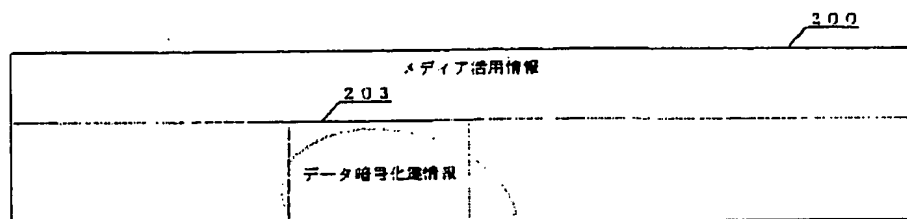
1707 映画作品名

- | | | | |
|------|--------------|------|------------|
| 1804 | 使用量累計 | 4512 | 送信データ暗号化手段 |
| 1805 | 最大使用量 | 4520 | 鍵管理サーバ |
| 3406 | 使用有効期限情報 | 4521 | 中央制御手段 |
| 4500 | DVD再生装置 | 4524 | 情報送受信手段 |
| 4501 | 中央制御手段 | 4525 | 情報記憶手段 |
| 4502 | 入力手段 | 4529 | ICカード |
| 4503 | 情報表示手段 | 4530 | ICカード駆動手段 |
| 4504 | 情報送受信手段 | 4531 | 受信データ復号化手段 |
| 4505 | 情報記憶手段 | 4532 | 送信データ暗号化手段 |
| 4506 | 映画作品DVD | 4533 | 乱数発生手段 |
| 4507 | DVD駆動手段 | 4534 | 利用者情報管理手段 |
| 4508 | DVD内データ復号化手段 | 4535 | DVD情報管理手段 |
| 4509 | ICカード | 4536 | 現在時刻発生手段 |
| 4510 | ICカード駆動手段 | 4537 | 使用有効期限判断手段 |
| 4511 | データ暗号化鍵復号化手段 | 4540 | ネットワーク |

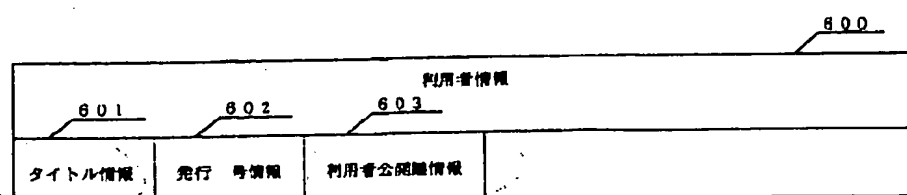
【図1】



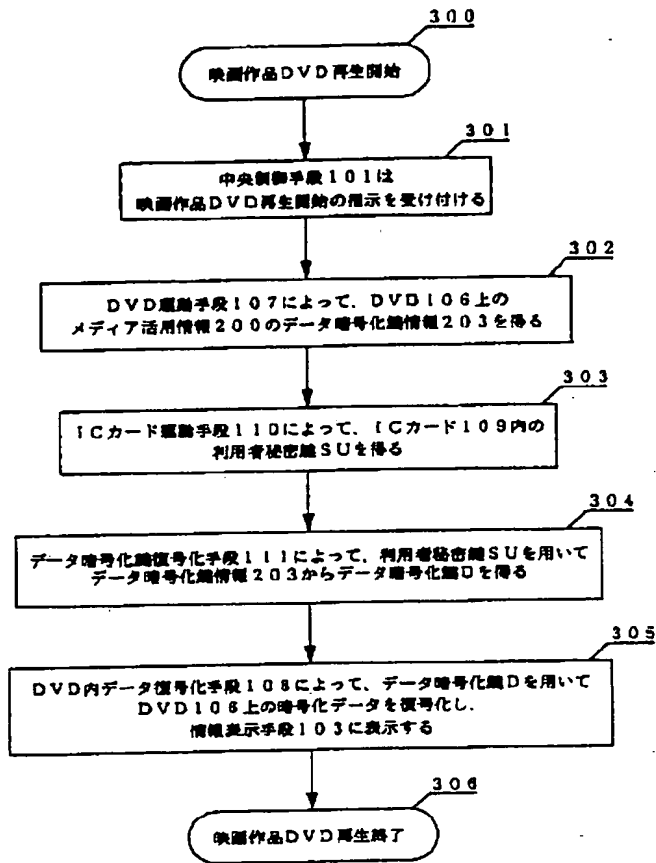
【図2】



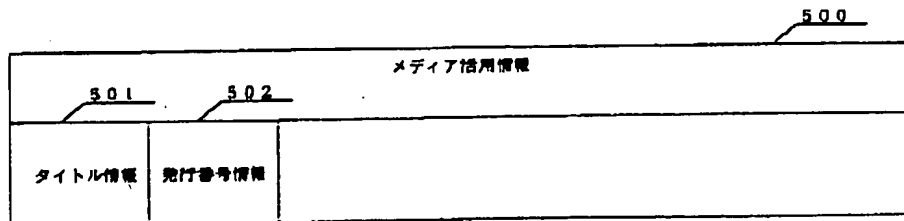
【図6】



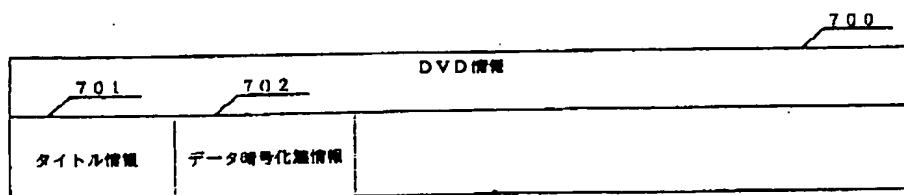
【図3】



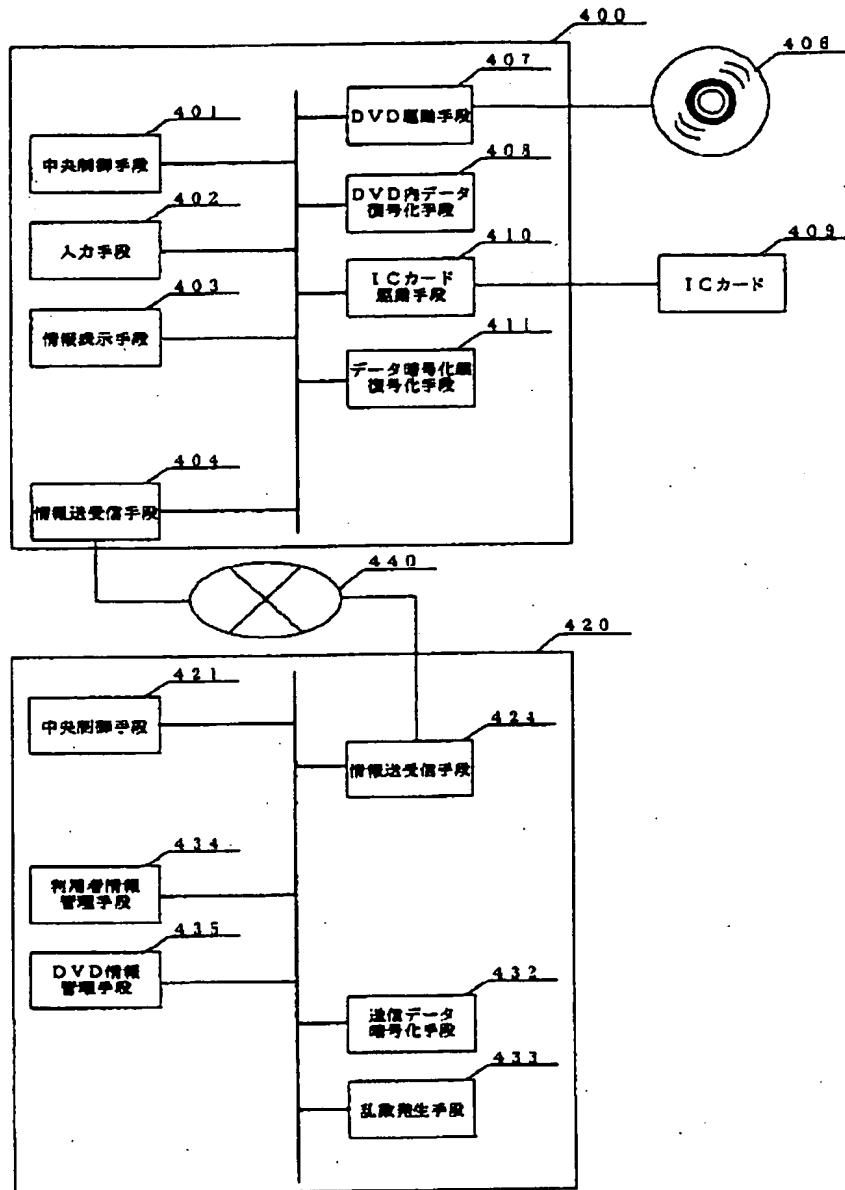
【図5】



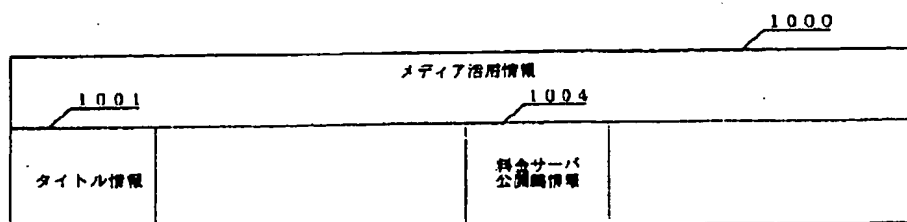
【図7】



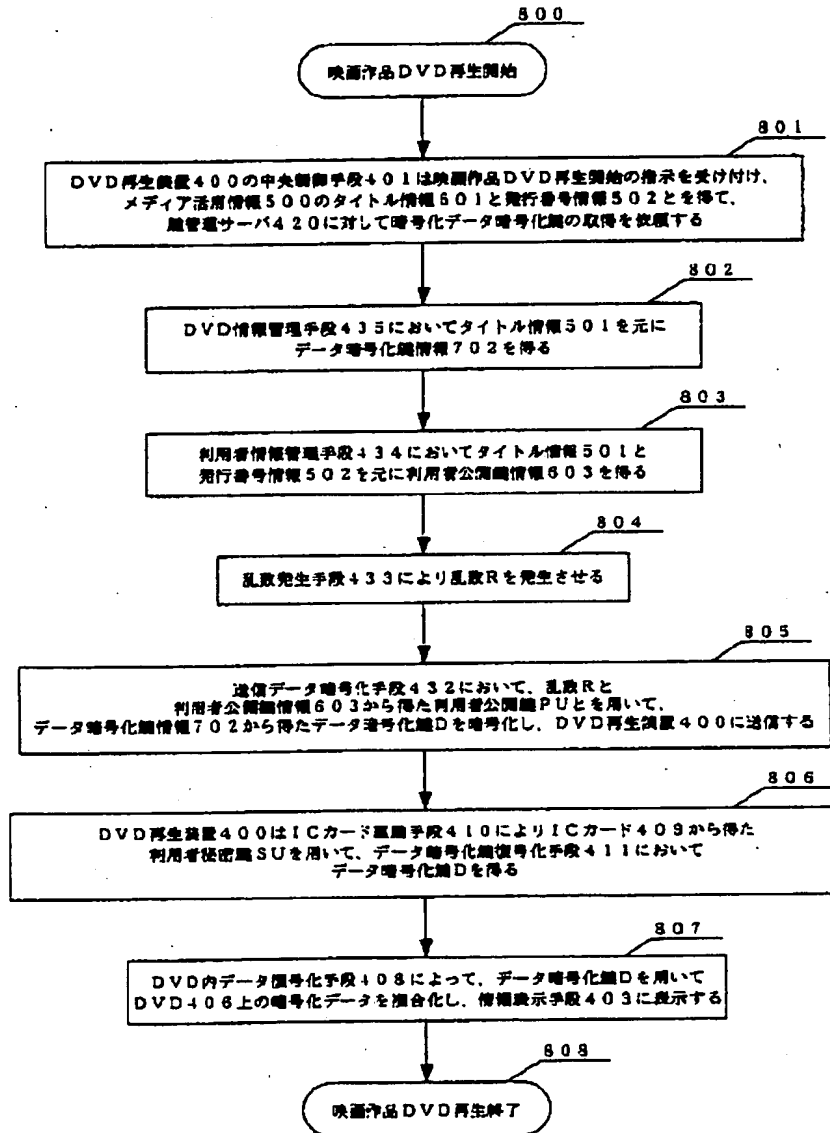
【図4】



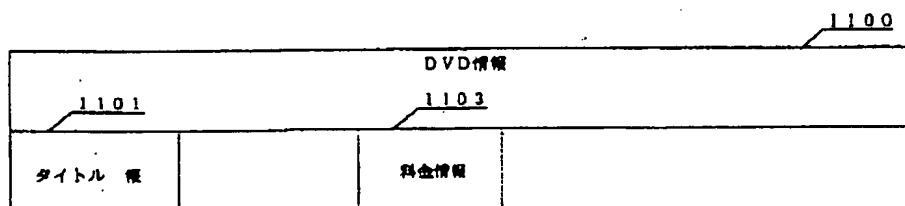
【図10】



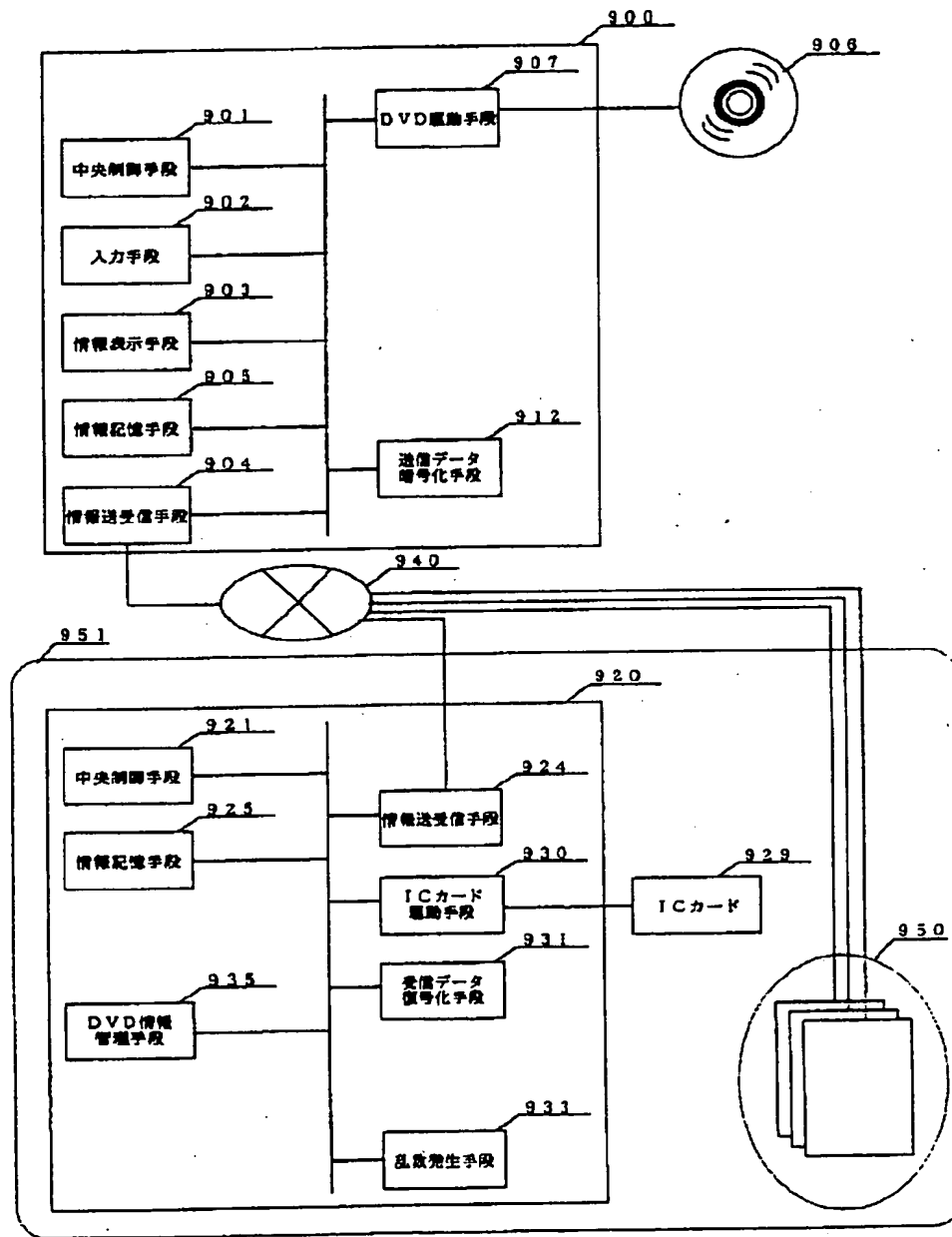
【図8】



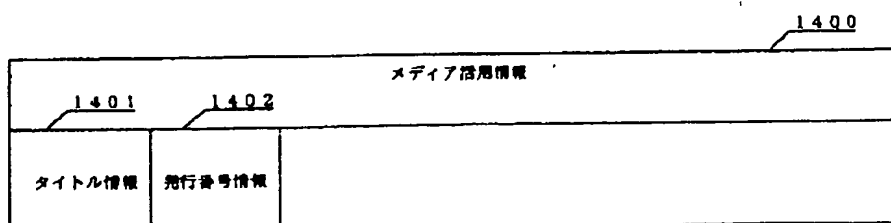
【図11】



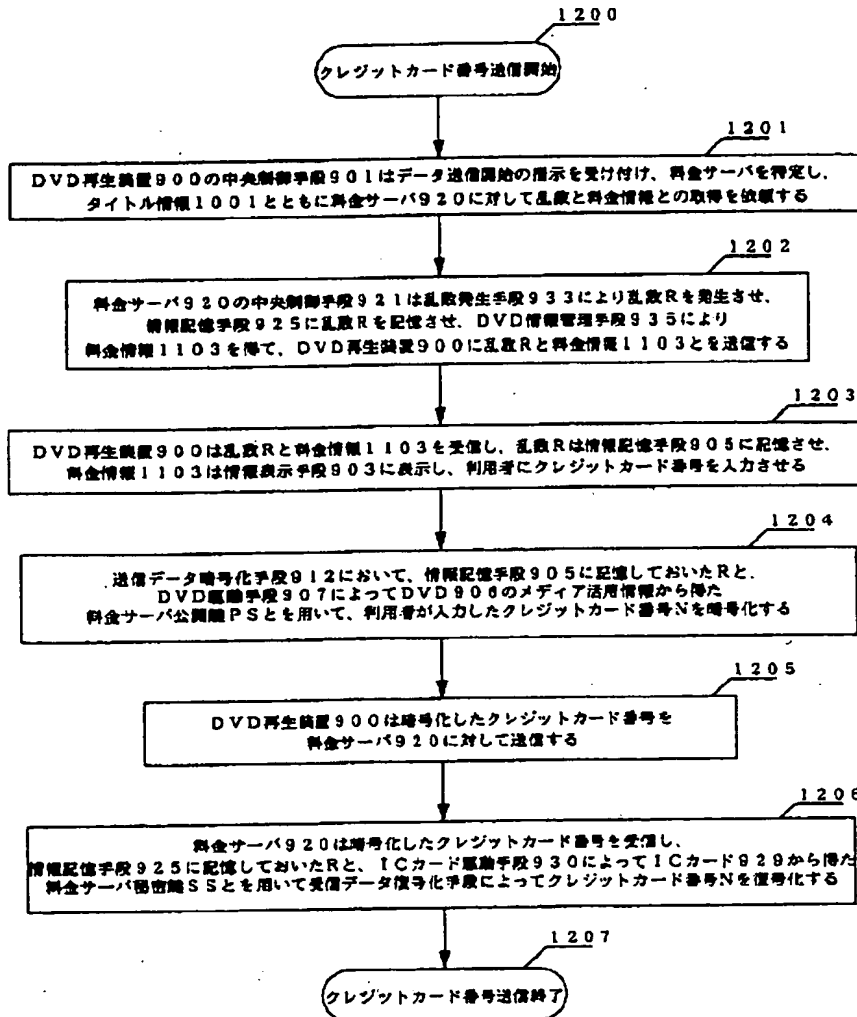
【図9】



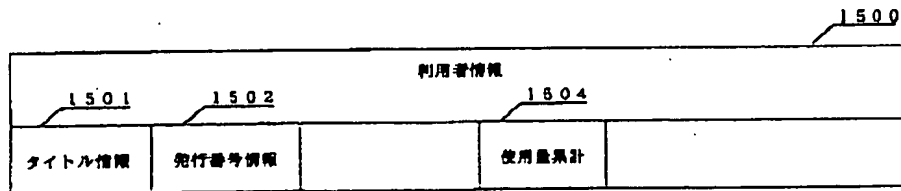
【図14】



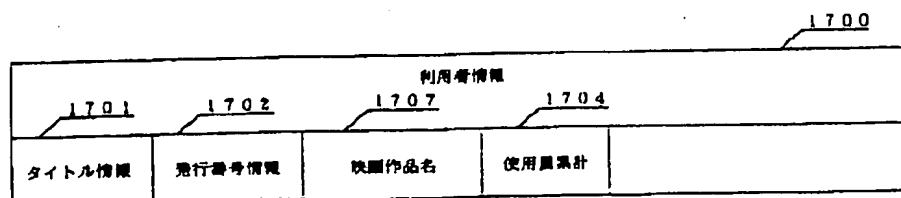
【図12】



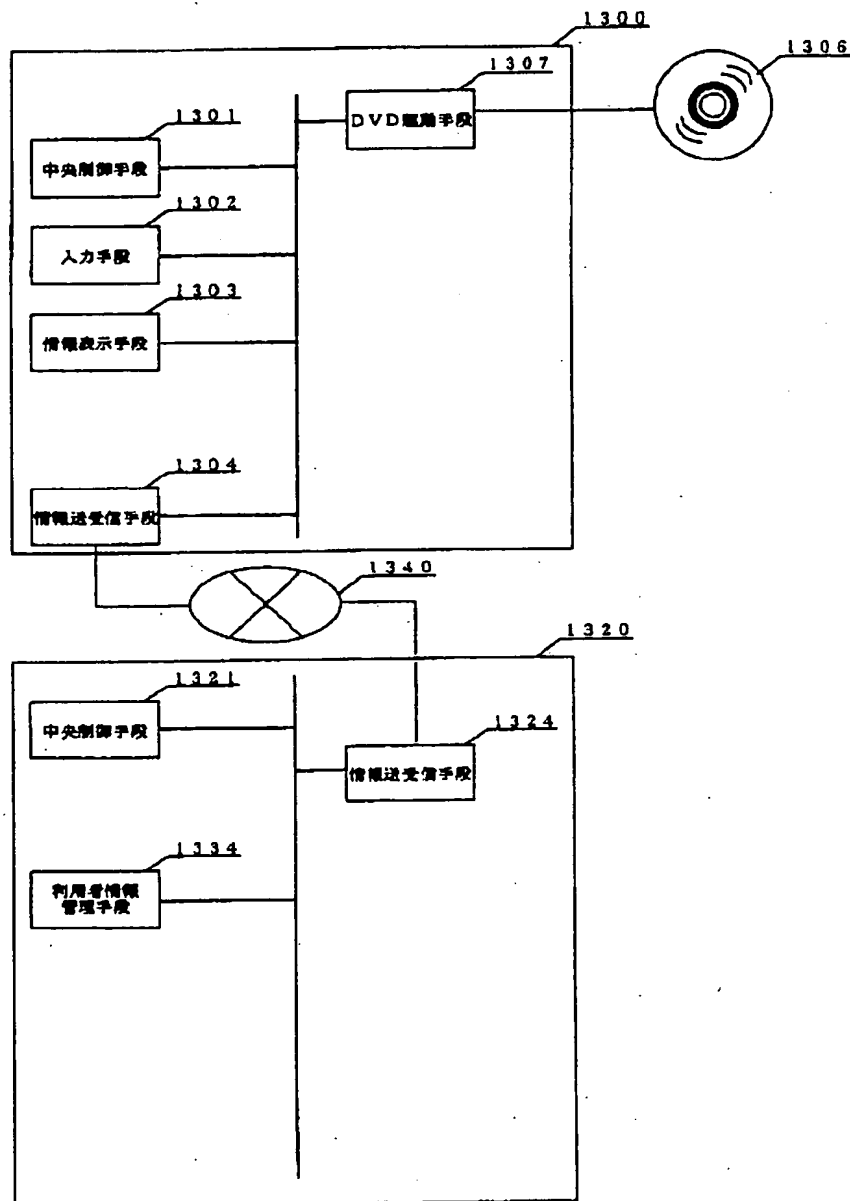
【図15】



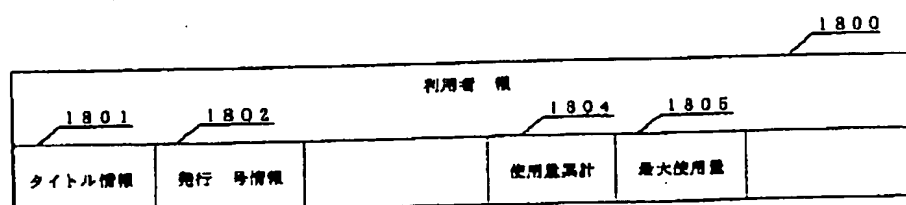
【図17】



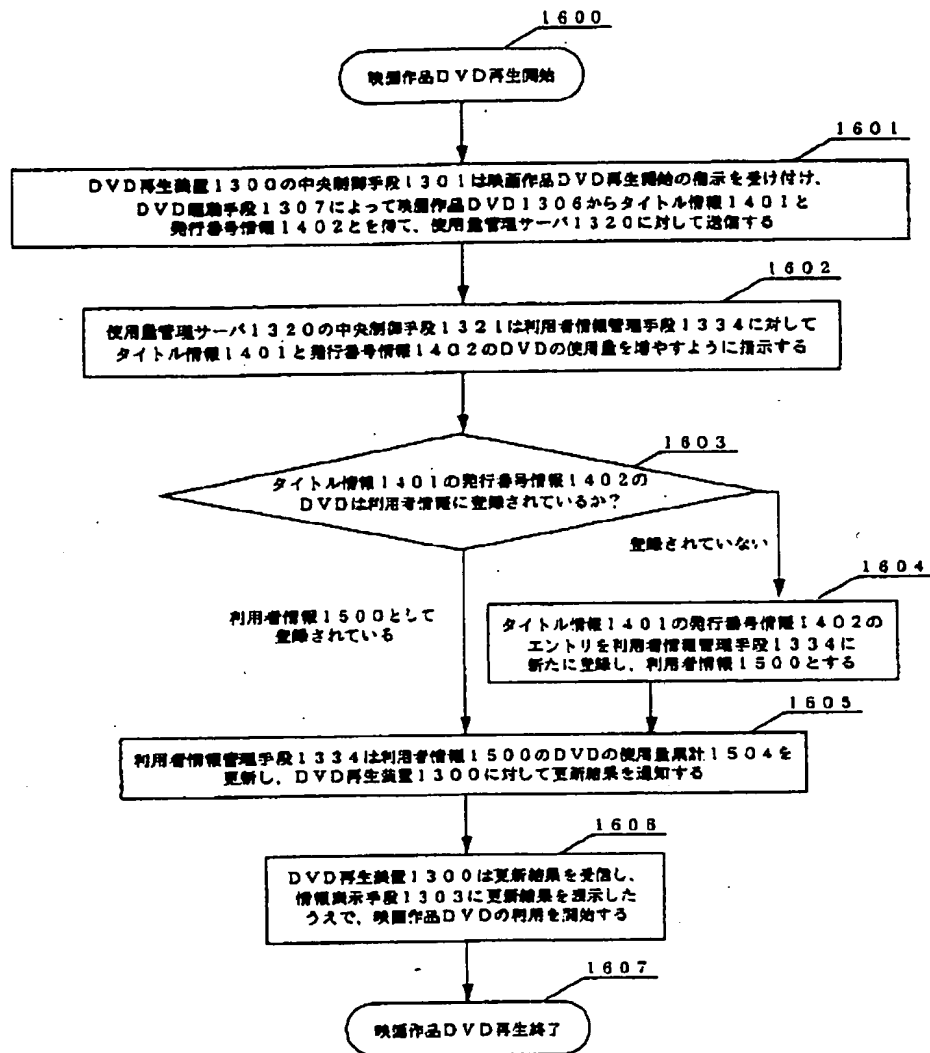
【図13】



【図18】



【図16】



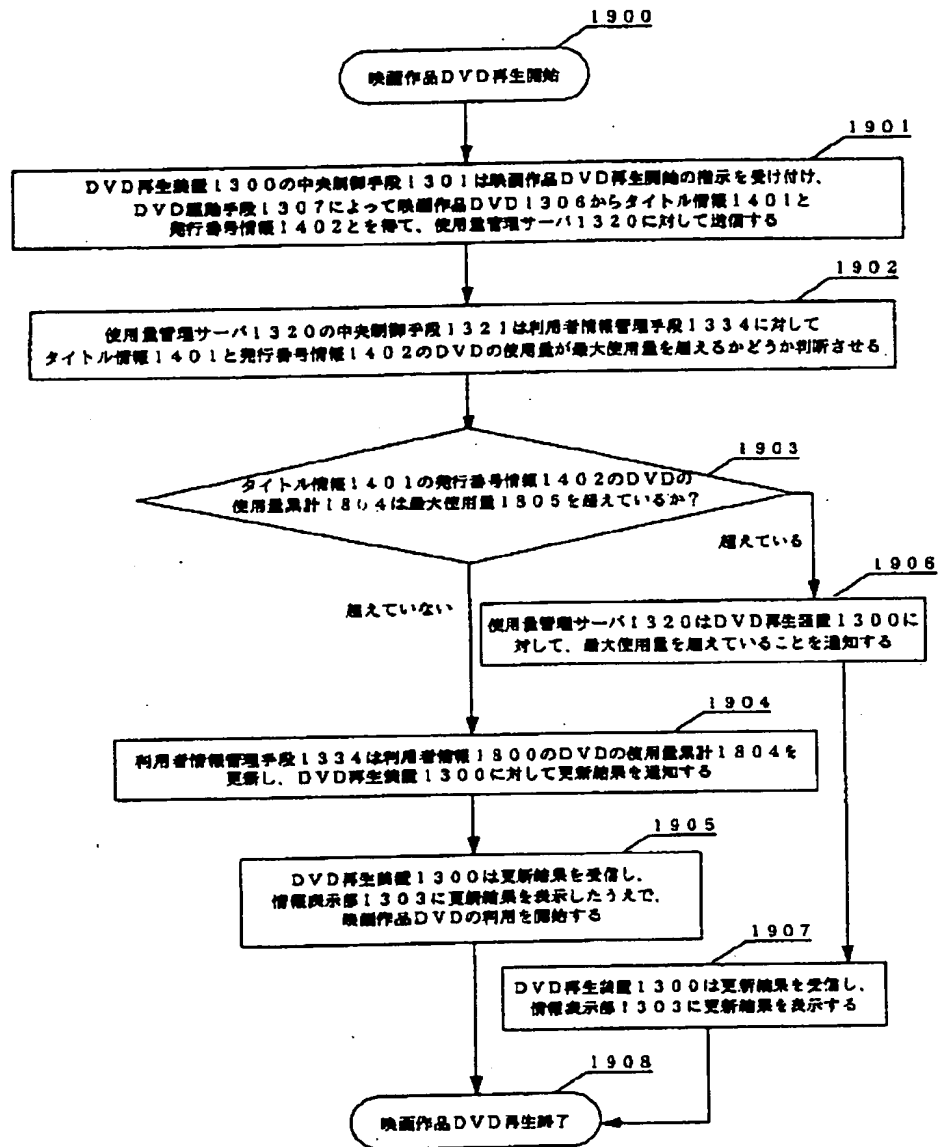
【図20】

| メディア借用情報 2000 | | | | |
|---------------|--------|------|-------|--|
| 2001 | 2002 | 2005 | | |
| タイトル情報 | 発行番号情報 | | 最大使用量 | |

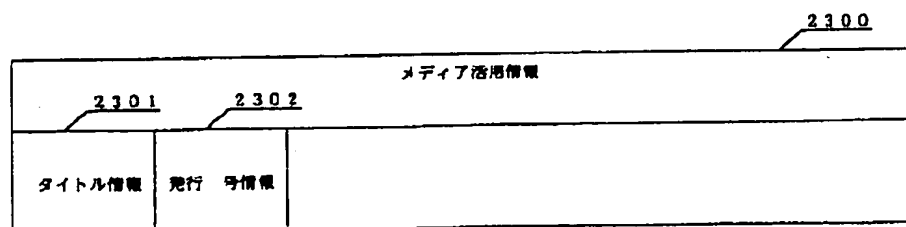
【図25】

| DVD情報 2500 | | |
|------------|-----------|--|
| 2501 | 2502 | |
| タイトル情報 | データ暗号化鍵情報 | |

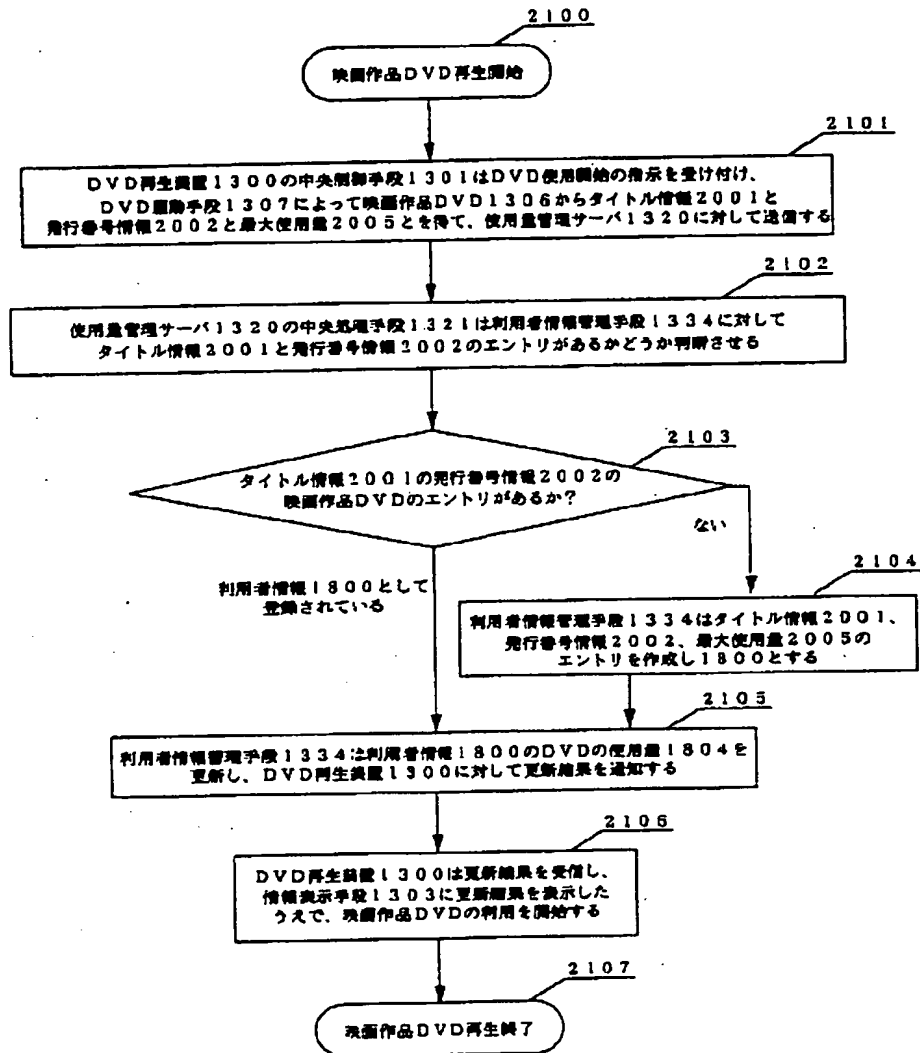
【図19】



【図23】



【図21】



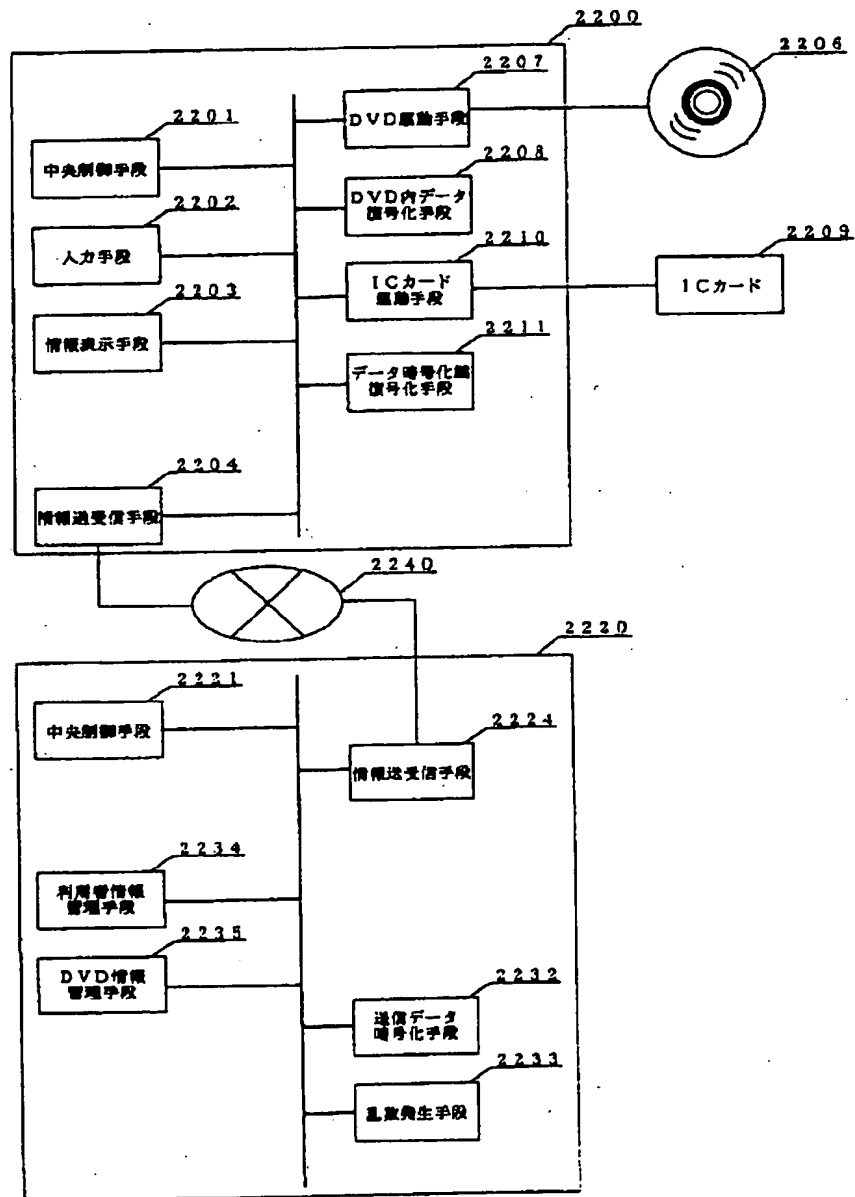
【図24】

| 2400 利用者情報 | | | | | |
|------------|--------|----------|-------|-------|--|
| 2401 | 2402 | 2403 | 2404 | 2405 | |
| タイトル情報 | 発行番号情報 | 利用者公開鍵情報 | 使用量累計 | 最大使用量 | |

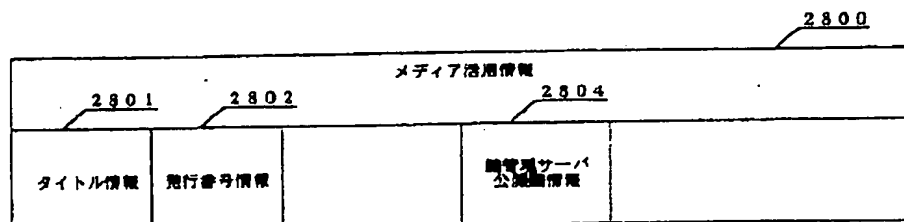
【図30】

| 3000 DVD情報 | | |
|------------|-----------|--|
| 3001 | 3002 | |
| タイトル情報 | データ暗号化鍵情報 | |

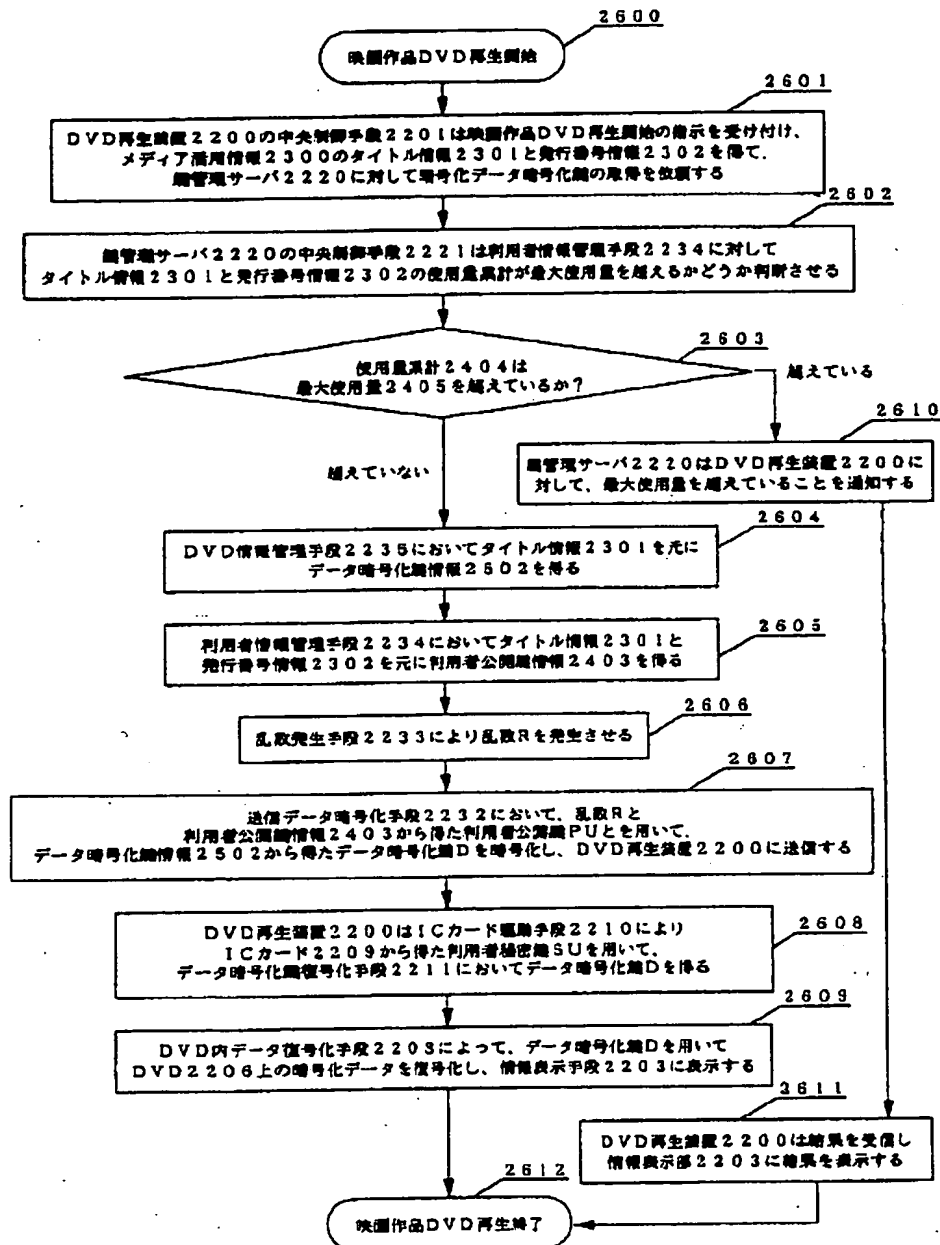
【図22】



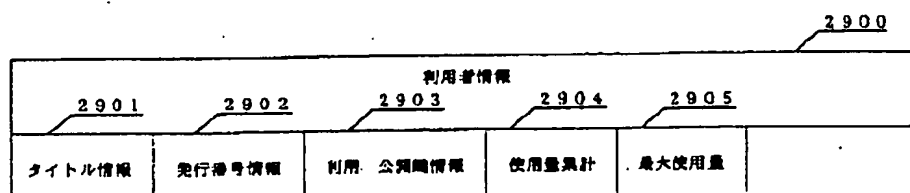
【図28】



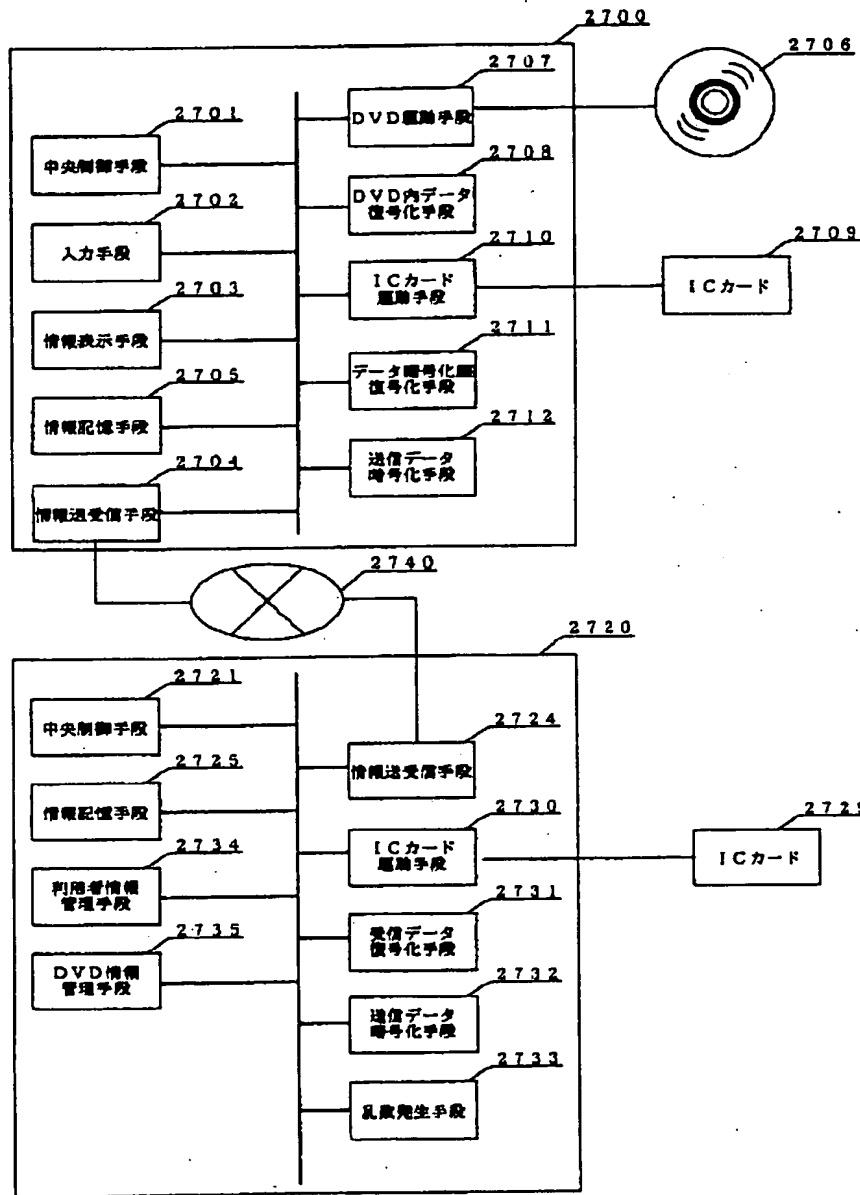
【図26】



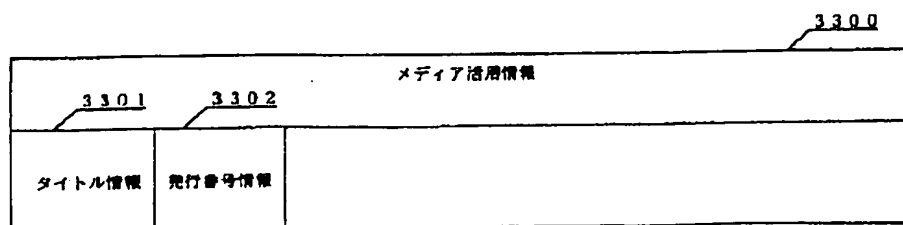
【図29】



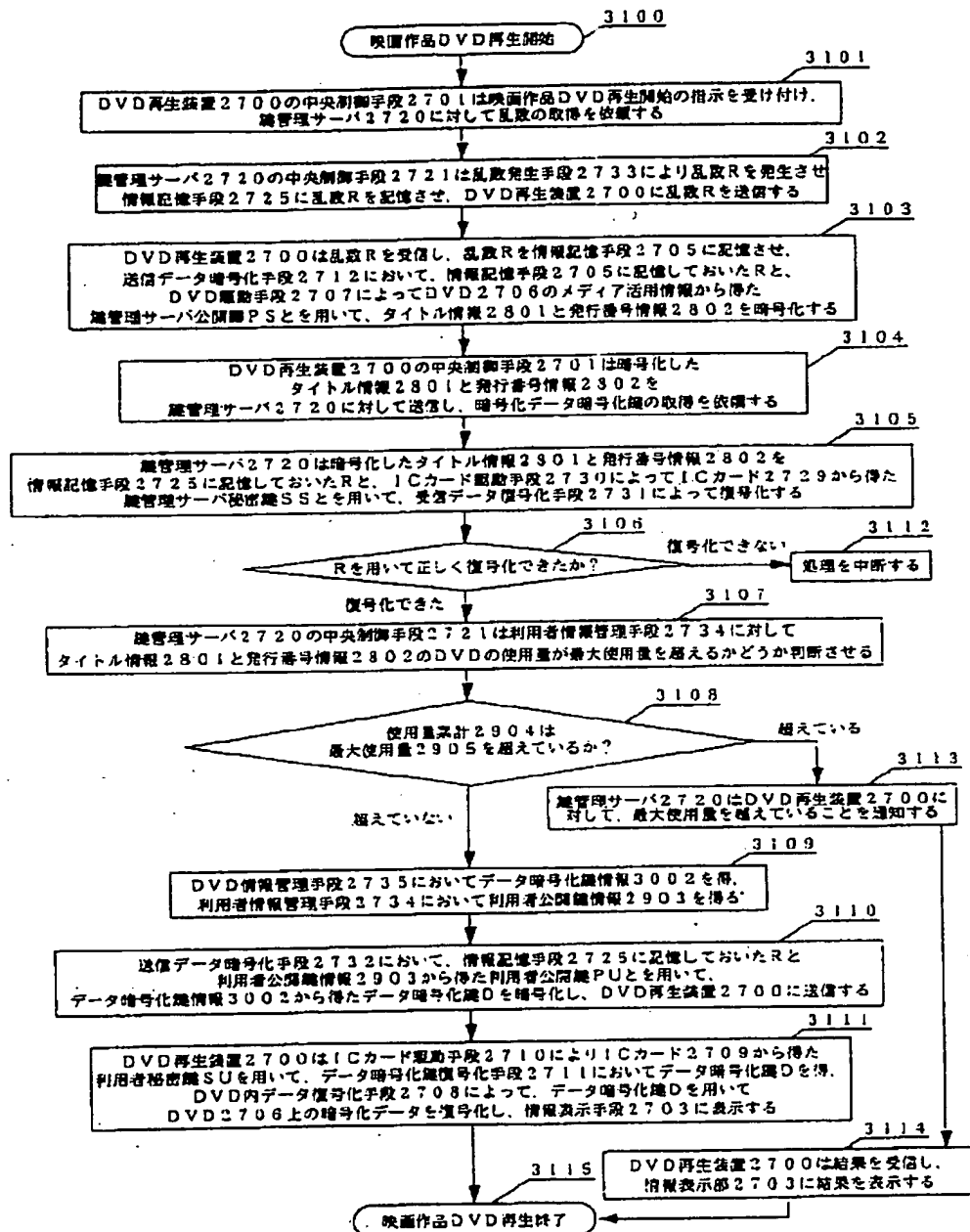
【図27】



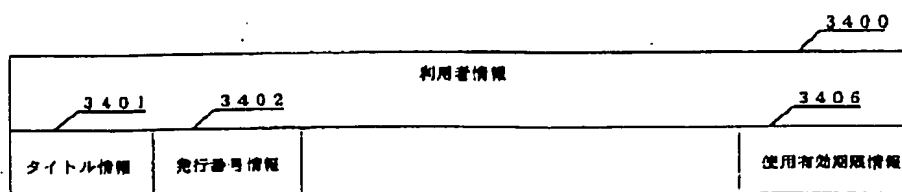
【図33】



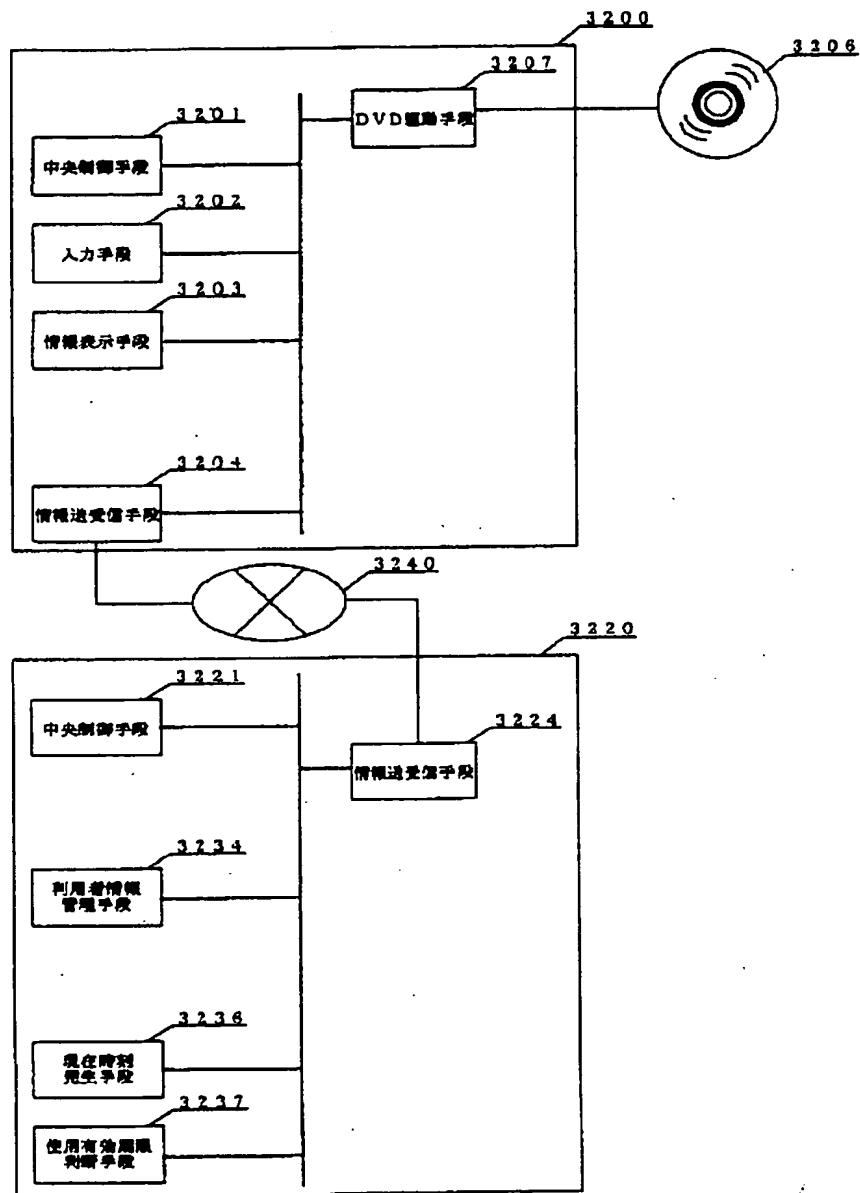
【図31】



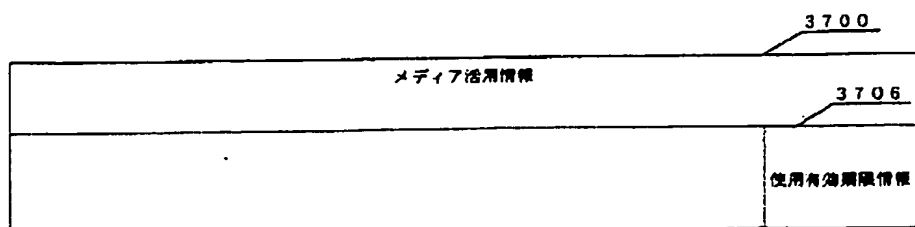
【図34】



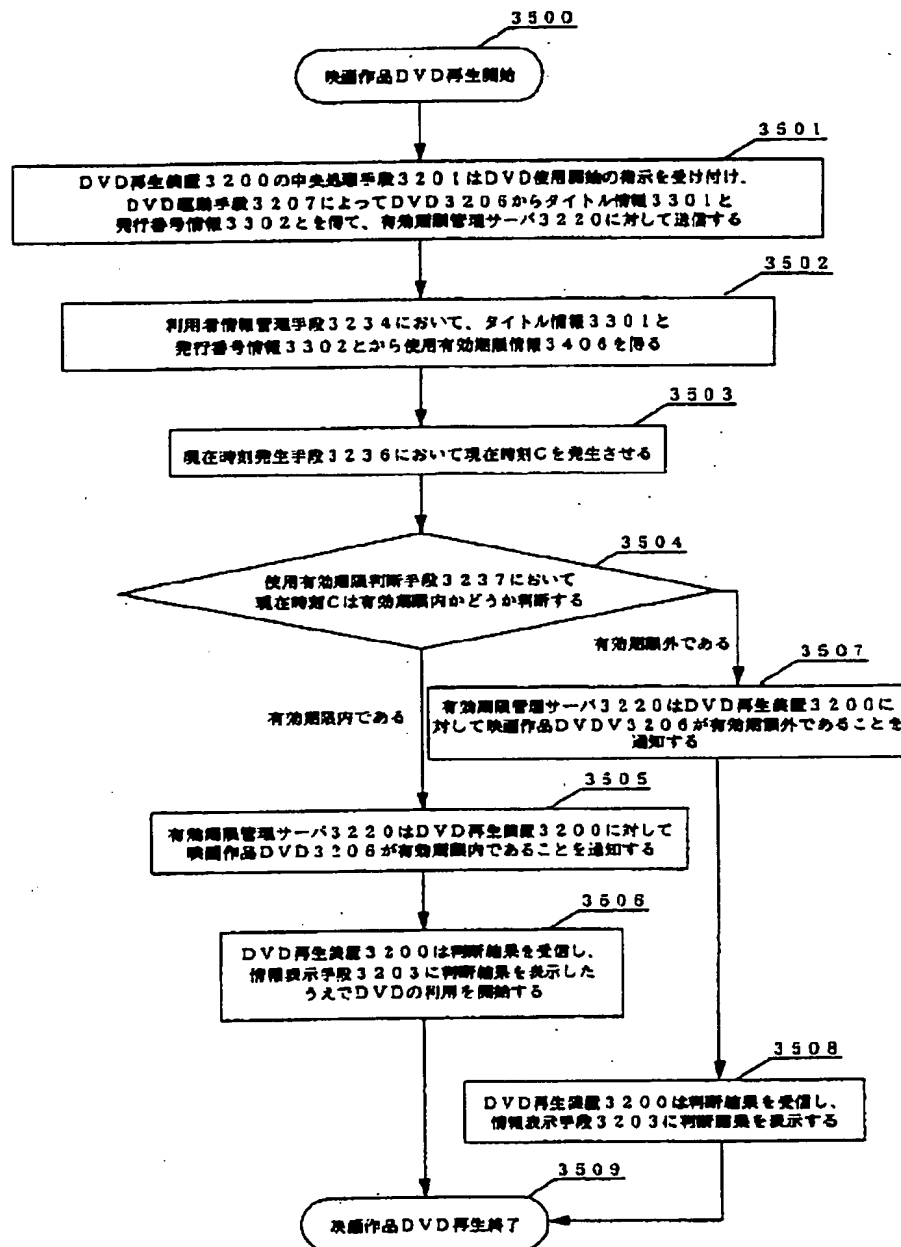
【図32】



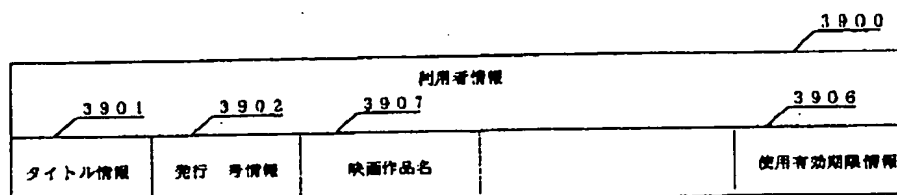
【図37】



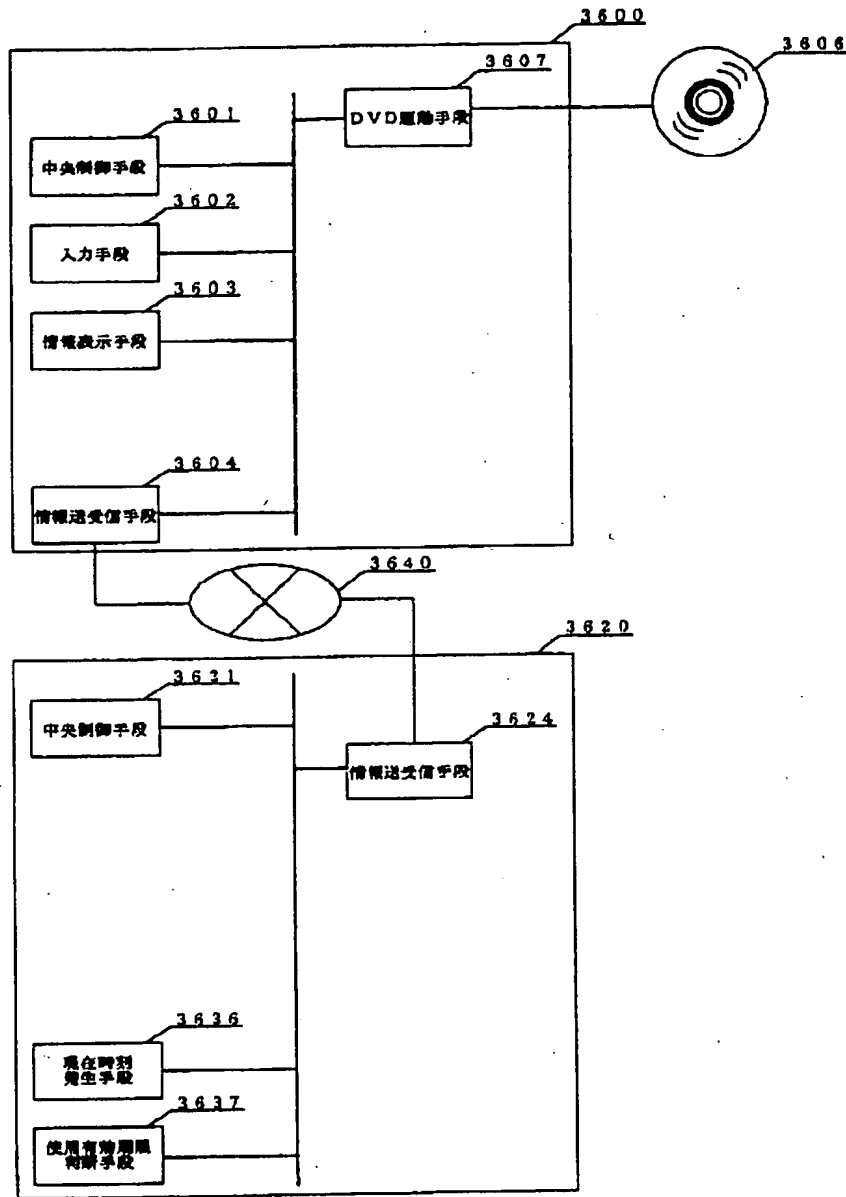
【図 35】



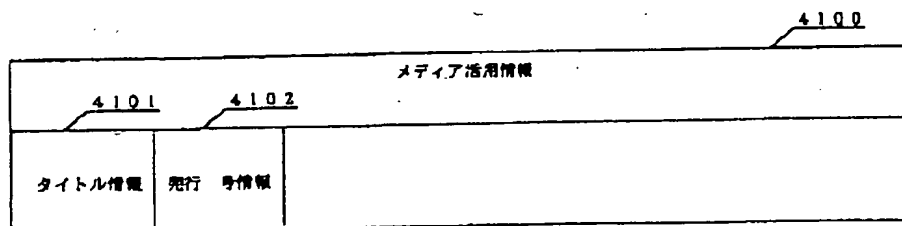
【図 39】



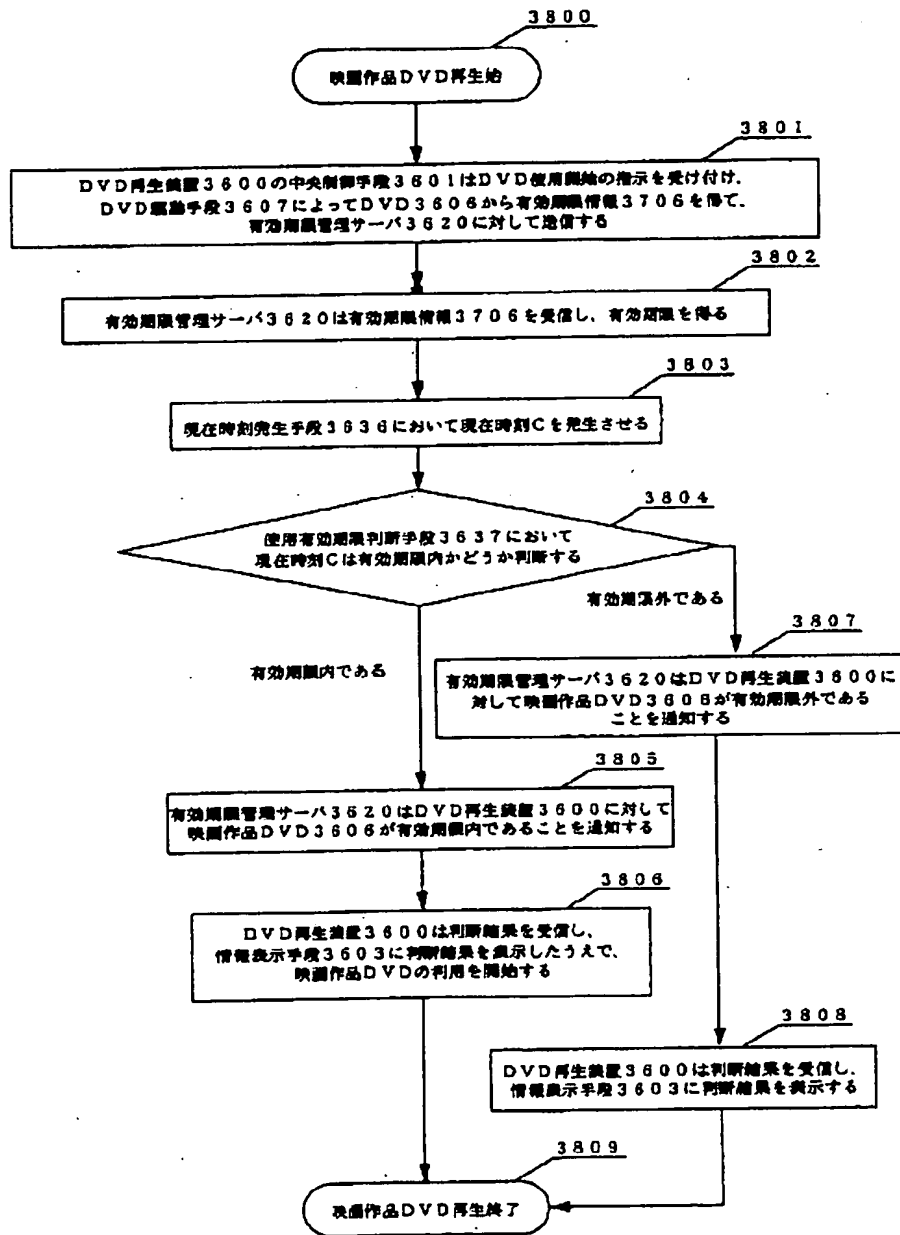
【図36】



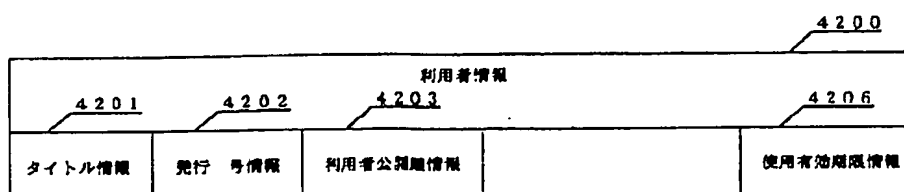
【図41】



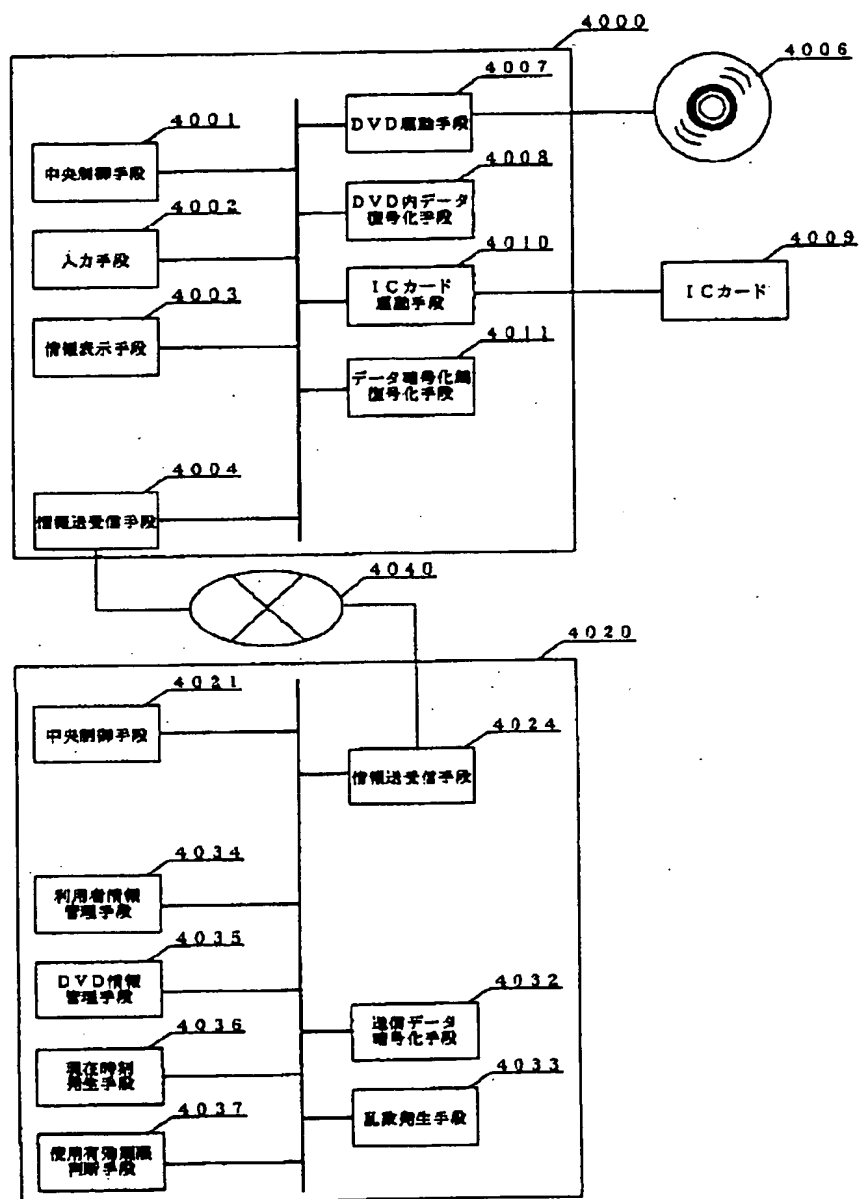
【図38】



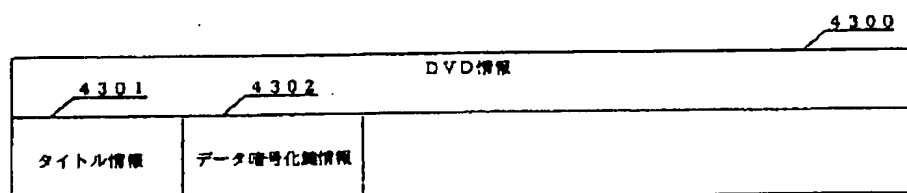
【図42】



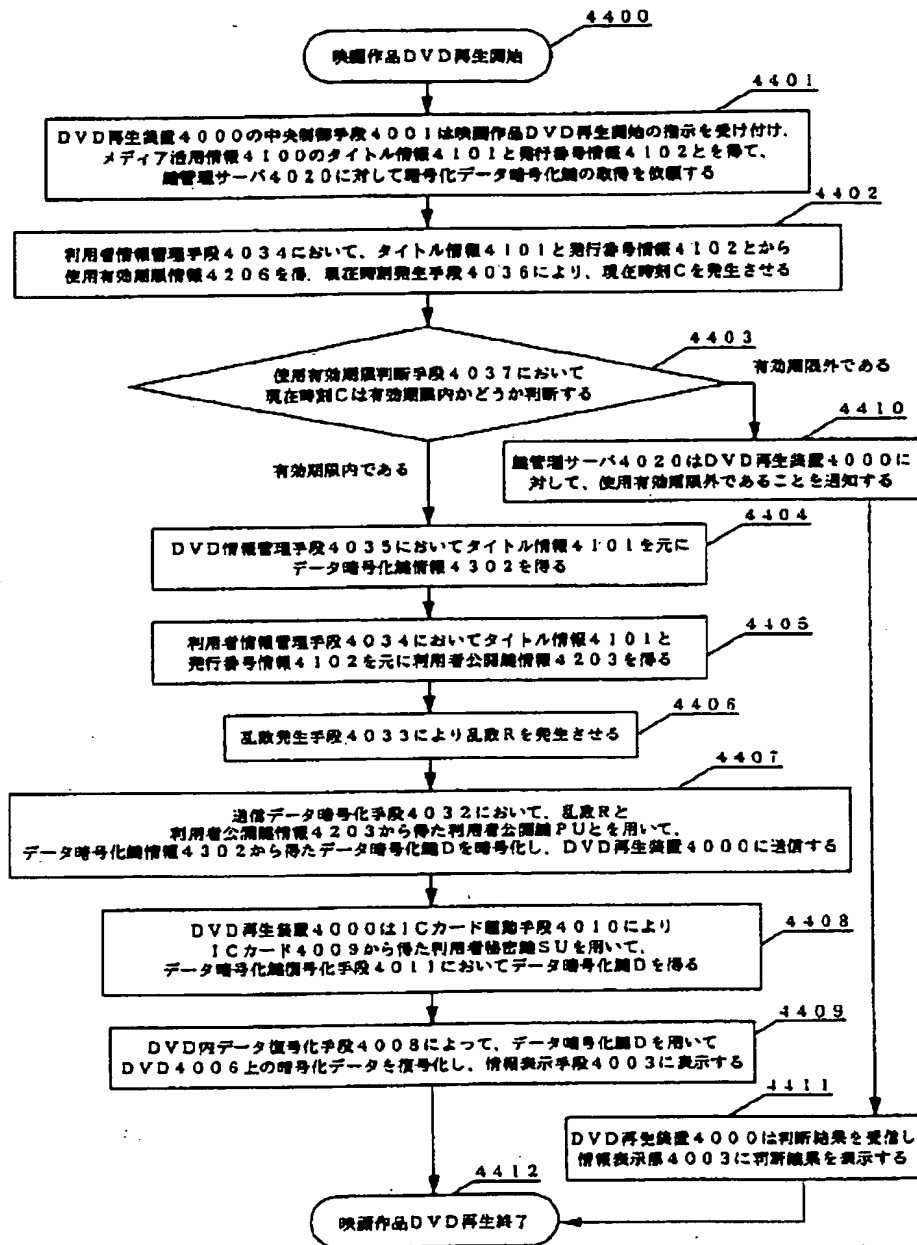
【図40】



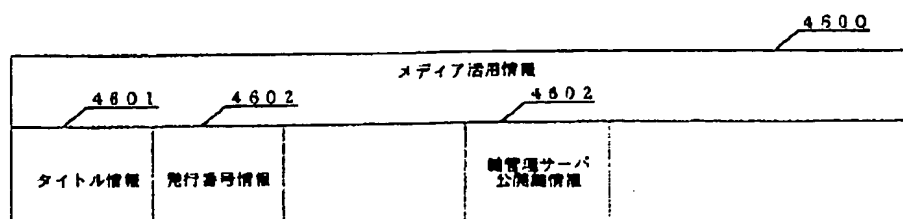
【図43】



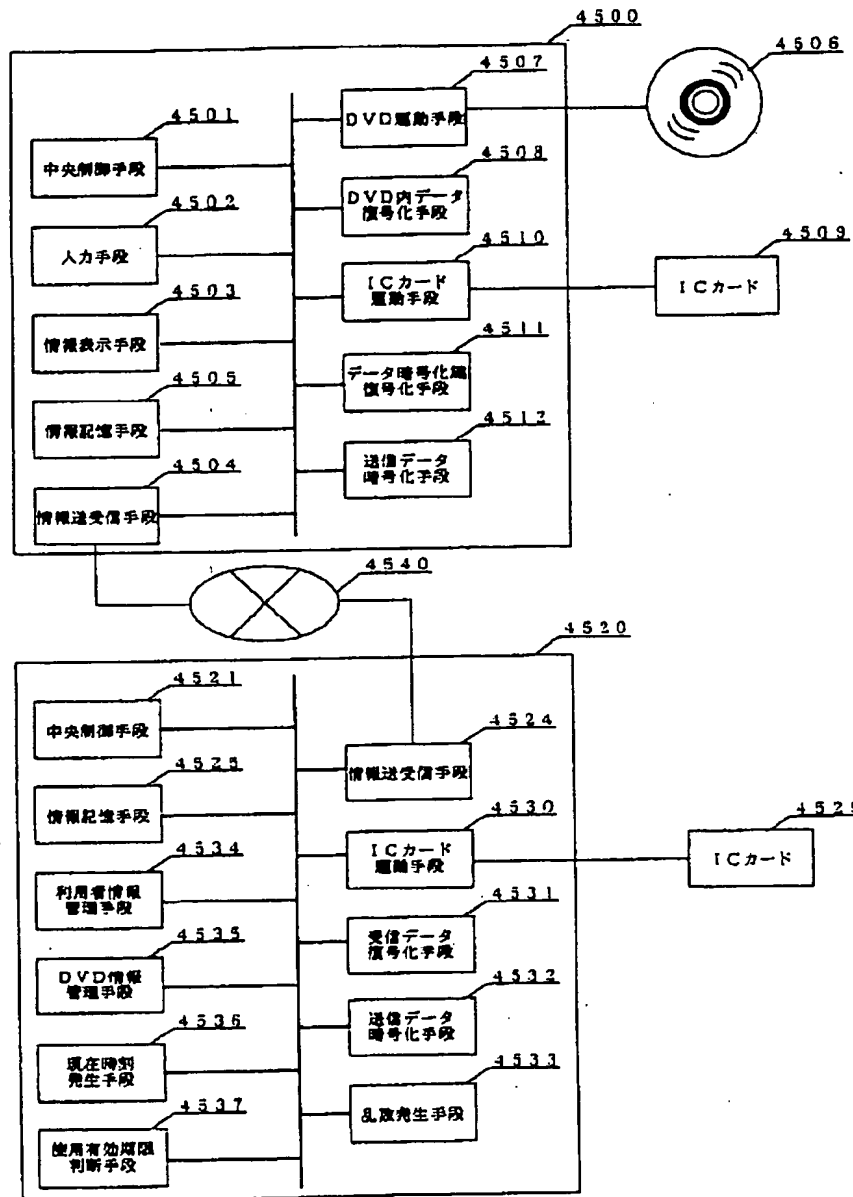
【図44】



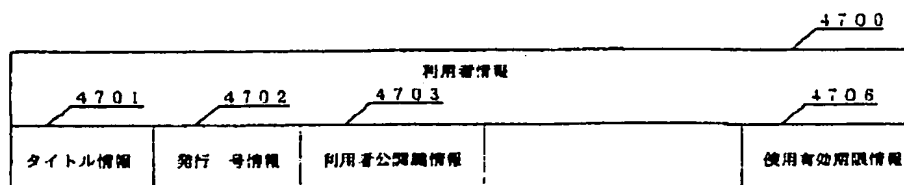
【図46】



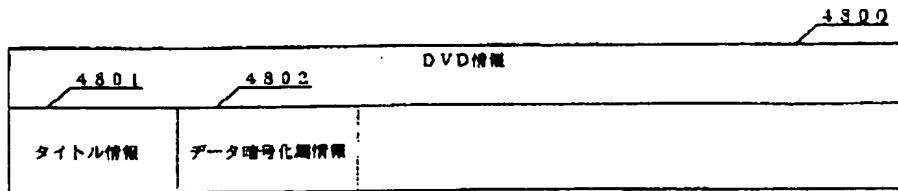
【図45】



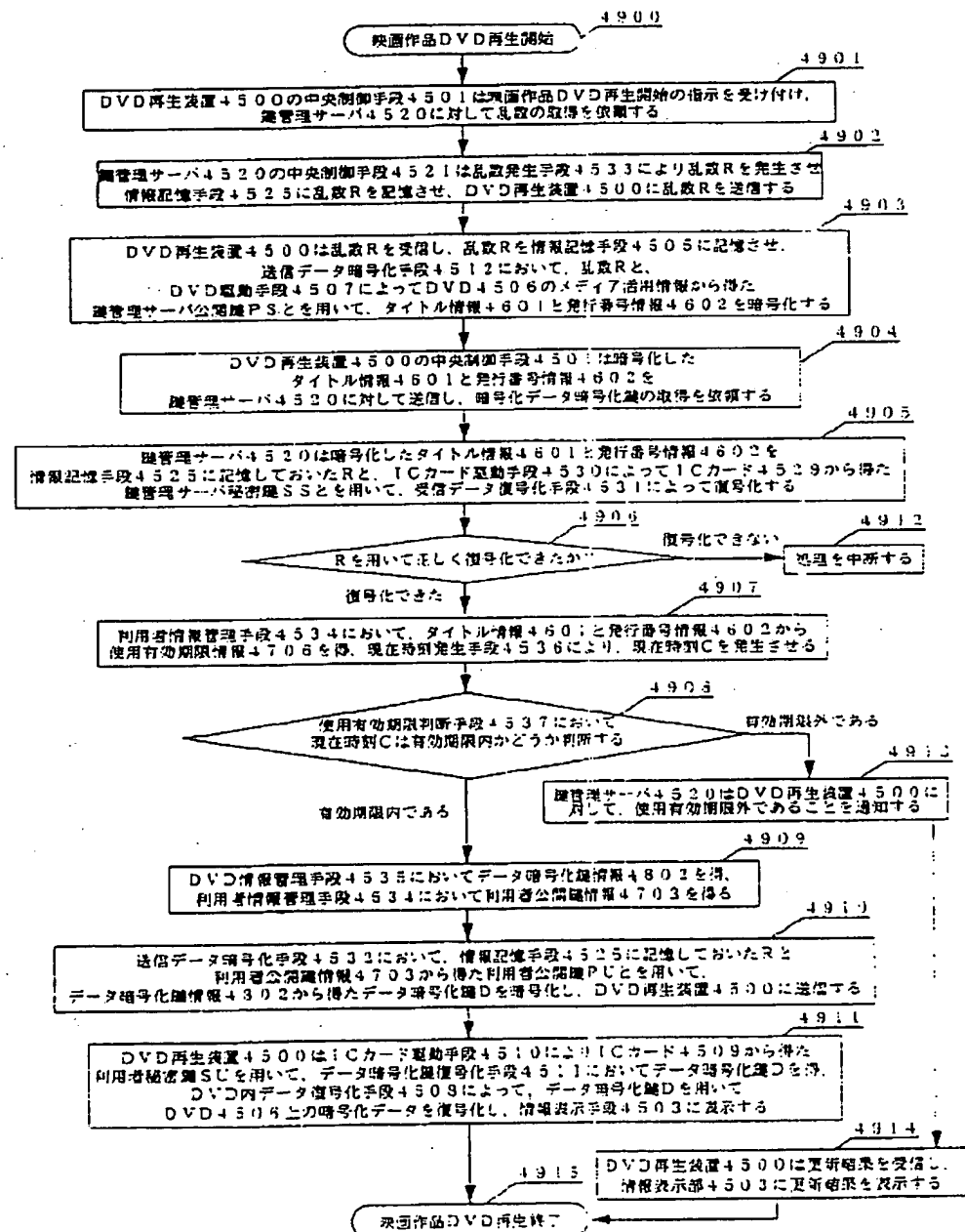
【図47】



【図48】



【図49】



フロントページの続き

(51) Int. Cl. ⁶

識別記号

F I

H 0 4 L 9/00

6 4 1